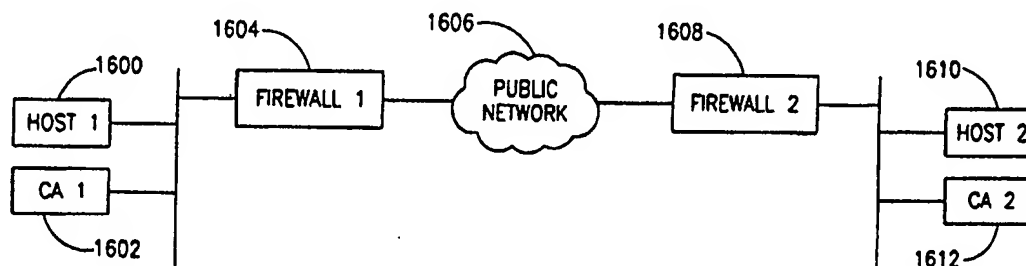




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04L 9/00, 12/56		A3	(11) International Publication Number: WO 97/00471
			(43) International Publication Date: 3 January 1997 (03.01.97)
(21) International Application Number: PCT/IL96/00017		(74) Agent: A. TALLY EITAN-ZEEV PEARL & CO.; Lumir House, 22 Maskit Street, 46733 Herzlia (IL).	
(22) International Filing Date: 16 June 1996 (16.06.96)			
(30) Priority Data: 114182 15 June 1995 (15.06.95) IL		(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).	
(60) Parent Application or Grant (63) Related by Continuation US 08/168,041 (CIP) Filed on 15 December 1993 (15.12.93)			
(71) Applicant (for all designated States except US): CHECK POINT SOFTWARE TECHNOLOGIES LTD. [IL/IL]; Ha-teomim Building 2, 35 Jabotinsky Street, 52511 Ramat Gan (IL).		Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>	
(72) Inventors; and (75) Inventors/Applicants (for US only): SHWED, Gil [IL/IL]; 21 Harechesh Street, 69699 Tel Aviv (IL). KRAMER, Shlomo [IL/IL]; 36 Harav Kuk Street, 63302 Tel Aviv (IL). ZUK, Nir [IL/IL]; 2 Zvi Street, 52504 Ramat Gan (IL). DOGON, Gil [IL/IL]; 78 Hakidma Street, 46743 Hertzlia (IL). BEN-REUVEN, Ehud [IL/IL]; 11 Arba Aratzot Street, 62486 Tel Aviv (IL).		(88) Date of publication of the international search report: 6 March 1997 (06.03.97)	

(54) Title: A SYSTEM FOR SECURING THE FLOW OF AND SELECTIVELY MODIFYING PACKETS IN A COMPUTER NETWORK



(57) Abstract

A novel system for controlling the inbound and outbound data packet flow in a computer network by which private networks can be secured from outside attacks. A user generates a rule base (400) which is converted into a set of filter language instructions where each rule includes a source, destination, service, whether to accept or reject the packet and whether to log the event. The filter language instructions are executed on inspection engines (204) on computers acting as firewalls (124) positioned in the network such that all traffic is forced to pass through the firewall. Packets are filtered in accordance with the rule base. The inspection engine acts as a virtual packet filter machine (600) determining whether to accept or reject a packet. If a packet is rejected, it is dropped, and if accepted may be modified. Modifications, performed in accordance with the rule base, may include encryption, decryption, signature generation or verification, or address translation.

(51) Int.Cl.⁶
 H 0 4 L 12/56
 G 0 9 C 1/00
 H 0 4 L 9/36

識別記号

6 6 0

F I

H 0 4 L 11/20

G 0 9 C 1/00

H 0 4 L 9/00

1 0 2 Z

6 6 0 E

6 8 5

審査請求 未請求 予備審査請求 有 (全 77 頁)

(21) 出願番号 特願平9-502876
 (86) (22) 出願日 平成8年(1996) 6月16日
 (85) 翻訳文提出日 平成9年(1997) 2月17日
 (86) 国際出願番号 P C T / I L 9 6 / 0 0 0 1 7
 (87) 国際公開番号 W O 9 7 / 0 0 4 7 1
 (87) 国際公開日 平成9年(1997) 1月3日
 (31) 優先権主張番号 1 1 4 1 8 2
 (32) 優先日 1995年6月15日
 (33) 優先権主張国 イスラエル (I L)

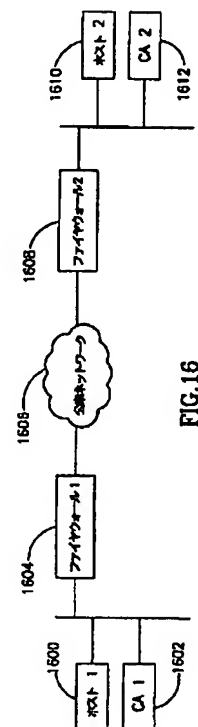
(71) 出願人 チェックポイント・ソフトウェア・テクノロジー・リミテッド
 イスラエル国ラマツガン52520・ヤボチ
 ンスキー ストリートヤハロンタワー 3
 エイ
 (72) 発明者 シュウェド、ギル
 イスラエル国テルアビブ69699・ハレチェ
 シュストリート 21
 (72) 発明者 クレイマー、シュロモ
 イスラエル国テルアビブ63302・ハラブク
 クストリート 36
 (74) 代理人 弁理士 大島 陽一 (外1名)

最終頁に続く

(54) 【発明の名称】 コンピュータネットワークにおける通信のセキュリティのためのデータパケットを検査し選択的
 変更を施す方法及びシステム及びそのシステムの操作方法

(57) 【要約】

本発明は、コンピュータネットワークにおける到着及び
 発信データパケットフローを制御するための新規なシス
 テムを開示するものである。コンピュータネットワーク
 におけるパケットフローを制御することによって、私設
 ネットワークから外界へのパケットフローを制御すると
 ともに、私設ネットワークを外部からの不法な攻撃から
 保護し得る。ユーザはルールベースを生成し、このルー
 ルベースは一組のフィルタリング処理言語命令セットに
 変換される。このルールベースの各ルールは、ソース、
 デスティネーション、サービス、パケットを通過させる
 か拒絶するか、及びイベントを記録するか否かを定める
 データを含んでいる。このフィルタリング処理言語命令
 セットは、コンピュータ上に設置された検査エンジンに
 インストールされ、その上で実行されて、ファイアウォ
 ールとして機能する。このファイアウォールは、ネット
 ワーク内を行き来する機密保護されるべき全てのトラヒ
 ックがこのファイアウォールを通過せざるを得ないよう
 に、コンピュータネットワーク内に設置される。従っ
 て、パケットは、ネットワークに出入りするときにルー



【特許請求の範囲】

1. コンピュータネットワークにおける到着及び発信データパケットを、セキュリティールに従って検査し選択的変更を施す方法であって、

前記セキュリティールによって検査された前記コンピュータネットワークの各アスペクトの定義を生成する過程と、

前記アスペクトの定義によって、前記アスペクトの少なくとも1つを制御する前記セキュリティールを生成する過程と、

前記セキュリティールを、前記セキュリティールに従って前記データパケットを検査し選択的変更を施すパケットフィルタリングモジュールの動作を制御するためのパケットフィルタリング処理言語命令セットに変換するセキュリティール変換過程と、

前記セキュリティールに従って前記データパケットを検査し選択的変更を施すために、仮想パケットフィルタリングマシンを実現する前記パケットフィルタリングモジュールと、前記コンピュータネットワークを接続する過程と、

前記パケットフィルタモジュールが前記パケットフィルタリング処理言語命令を実行して前記仮想パケットフィルタリングマシンを操作し、前記コンピュータネットワークから、または前記コンピュータネットワークへの前記データパケットの出入りを受容若しくは拒絶し、そのようにして受容された前記データパケットを選択的変更を施すパケットフィルタリング処理言語命令実行過程とを有することを特徴とするコンピュータネットワークにおける到着及び発信データパケットを、セキュリティールに従って検査し選択的変更を施す方法。

2. 前記アスペクトが、ネットワークオブジェクトを含むことを特徴とする請求項1に記載の方法。

3. 前記アスペクトが、ネットワークサービスを含むことを特徴とする

請求項1に記載の方法。

4. 前記アスペクトが、ネットワークサービスを含むことを特徴とする請求項2に記載の方法。

5. 前記アスペクトたる前記オブジェクトの定義が、前記オブジェクトのアドレ

スを含むことを特徴とする請求項4に記載の方法。

6. 前記セキュリティール変換過程の前記フィルタリング処理言語命令セットが、スクリプトの形態であり、前記スクリプトを、前記パケットフィルタリング処理言語命令実行過程において実行される前記命令セットにコンパイルするコンパイラを含んでいることを特徴とする請求項1に記載の方法。

7. 前記コンピュータネットワークの各アスペクトの定義を生成する過程、及び前記セキュリティールを生成する過程の双方において、グラフィカルな定義がなされることを特徴とする請求項1に記載の方法。

8. 前記選択的変更が、暗号化、復号化、署名生成、及び署名確認からなる処理のグループから選択されることを特徴とする請求項1に記載の方法。

9. コンピュータネットワークにおける到着及び発信データパケットを、セキュリティールに従って検査し選択的変更を施すセキュリティシステムであって、前記セキュリティールによって検査される前記コンピュータネットワークの各アスペクトが予め定義されており、前記セキュリティールが前記アスペクトによって前もって定義されており、かつパケットフィルタリング処理言語命令に変換される、該セキュリティシステムを操作する方法において、

前記セキュリティールによって検査される前記コンピュータネットワークの少なくとも1つのエンティティにおいて、前記コンピュータネットワークに接続されたパケットフィルタリングモジュールを設ける過

程であって、前記パケットフィルタリングモジュールが、前記コンピュータネットワークに、または前記コンピュータネットワークから出入りする前記データパケットを検査し選択的変更を施す仮想パケットフィルタリングマシンを実現する、該過程と、

前記パケットフィルタモジュールが前記パケットフィルタリング処理言語命令を実行して前記仮想パケットフィルタリングマシンを操作し、前記コンピュータネットワークから、または前記コンピュータネットワークへの前記データパケットの出入りを受容若しくは拒絶し、そのようにして受容された前記データパケットを選択的変更を施すパケットフィルタリング処理言語命令実行過程とを有する

ことを特徴とするセキュリティシステムを操作する方法。

10. 前記アスペクトが、ネットワークオブジェクトを含むことを特徴とする請求項9に記載の方法。

11. 前記アスペクトが、ネットワークサービスを含むことを特徴とする請求項9に記載の方法。

12. 前記アスペクトが、ネットワークサービスを含むことを特徴とする請求項10に記載の方法。

13. 前記アスペクトたる前記オブジェクトの定義が、前記オブジェクトのアドレスを含むことを特徴とする請求項12に記載の方法。

14. 前記仮想パケットフィルタリングマシンが、データ抽出操作を実行することを特徴とする請求項9に記載の方法。

15. 前記仮想パケットフィルタリングマシンが、論理演算を実行することを特徴とする請求項14に記載の方法。

16. 前記仮想パケットフィルタリングマシンが、比較処理を実行することを特徴とする請求項15に記載の方法。

17. 前記選択的変更が、暗号化、復号化、署名生成、及び署名確認か

らなる処理のグループから選択されることを特徴とする請求項9に記載の方法。

18. コンピュータネットワークにおける到着及び発信データパケットを、セキュリティルールに従って検査し選択的変更を施すセキュリティシステムであって、前記セキュリティルールによって検査される前記コンピュータネットワークの各アスペクトが予め定義されており、前記セキュリティルールが前記アスペクトによって前もって定義されており、かつパケットフィルタリング処理言語命令に変換される、該セキュリティシステムを操作する方法において、

前記セキュリティルールによって検査される前記コンピュータネットワークの少なくとも1つのエンティティにおいて、前記コンピュータネットワークに接続されたパケットフィルタリングモジュールを設ける過程であって、前記パケットフィルタリングモジュールが、前記コンピュータネットワークに、または前記コンピュータネットワークから出入りする前記データパケットを検査し選択的変更

を施す仮想パケットフィルタリングマシンをエミュレートする、該過程と、

前記パケットフィルタリングモジュールが、パケットフィルタリング処理を実行するための前記パケットフィルタリング処理言語命令を読み出し、実行する過程と、

前記パケットフィルタリング処理言語命令を読み出し、実行する過程において得られた結果を記憶装置に格納する過程と、

前記パケットフィルタリングモジュールが、格納された前記結果を用いて、前記パケットフィルタリング処理言語命令に基づいた前記仮想パケットフィルタリングマシンの操作を行い、前記コンピュータネットワークから、または前記コンピュータネットワークへの前記データパケットの出入りを受容若しくは拒絶し、そのようにして受容された前記デー

タパケットを選択的変更を施す過程とを有することを特徴とするセキュリティシステムを操作する方法。

19. 前記アスペクトが、ネットワークオブジェクトを含むことを特徴とする請求項18に記載の方法。

20. 前記アスペクトが、ネットワークサービスを含むことを特徴とする請求項18に記載の方法。

21. 前記アスペクトが、ネットワークサービスを含むことを特徴とする請求項19に記載の方法。

22. 前記アスペクトたる前記オブジェクトの定義が、前記オブジェクトのアドレスを含むことを特徴とする請求項21に記載の方法。

23. 前記選択的変更が、暗号化、復号化、署名生成、及び署名確認からなる処理のグループから選択されることを特徴とする請求項18に記載の方法。

24. コンピュータネットワークを行き来する到着及び発信データパケットを、セキュリティルールに従って検査し選択的変更を施すセキュリティシステムであって、前記セキュリティルールによって制御される前記コンピュータネットワークの各アスペクトが予め定義されており、前記セキュリティルールが前記アスペクトによって前もって定義されており、かつパケットフィルタリング処理言語命

令に変換される、該セキュリティシステムにおいて、

前記セキュリティルールに従って動作し、前記コンピュータネットワークに、または前記コンピュータネットワークから出入りする前記データパケットを検査し選択的変更を施す仮想パケットフィルタリングマシンを実現する、前記コンピュータネットワークに接続されたパケットフィルタリングモジュールと、
前記パケットフィルタリング処理言語命令を読み出し実行する、前記

パケットフィルタリングモジュールと一体化された処理手段であって、前記パケットフィルタリングモジュールの操作を行い、前記コンピュータネットワークから、または前記コンピュータネットワークへの前記データパケットの出入りを受容若しくは拒絶し、そのようにして受容された前記データパケットを選択的変更を施す、該処理手段とを有することを特徴とするセキュリティシステム。

25. 前記選択的変更が、暗号化、復号化、署名生成、及び署名確認からなる処理のグループから選択されることを特徴とする請求項24に記載のセキュリティシステム。

26. 図面に記載された実施例と実質的に同一であることを特徴とする請求項1乃至23の何れか1つに記載の方法。

【発明の詳細な説明】

コンピュータネットワークにおける通信のセキュリティのためのデータパケットを検査し選択的変更を施す方法及びシステム及びそのシステムの操作方法

発明の背景

本出願は、一般に、コンピュータネットワークの機密保護、即ちセキュリティを制御する方法に関する。詳述すると、本出願は、外部及び内部のデスティネーション（終点）から、及びそこへ向かってネットワーク上を流れる情報を制御するコンピュータネットワークセキュリティのための、容易に変更可能、若しくは拡張可能な方法に関する。

接続性、即ちコネクティビティとセキュリティとは、多くの組織のコンピューティング環境における2つの両立困難な目的である。典型的な最近のコンピューティングシステムは、数多くのサービスに透過的にアクセスできるネットワーク通信網の周りに構築される。このようなサービスはグローバルに利用可能であり、これが最近のコンピューティングソリューションの唯一の最も重要な特徴であろう。接続性に対する要求は、組織内部及びその外部の双方から要求されているものである。

ネットワークサービスを無許可の使用から保護することは、全ての組織にとって非常に重要なことである。例えば、ユニックスワークステーションはひとたびインターネットに接続されると全世界に全てのサービスを提供し、そのサービスは次のテーブル上の別のステーションにも提供される。現在の技術を用いると、1つの組織は不正アクセスに対する防備のために、外界または他のサイトへの全ての接続が不可能になるほどその接続性を犠牲にしなければならない。

高度なセキュリティの必要性が高まるにつれ、ネットワークリソース

へのアクセスを制御する手段が管理上の優先すべき事項となってきた。また、コストを節約し、生産性を維持するために、アクセスコントロールは、単純に校正でき、ユーザ及びアプリケーションに対して透過的なものでなければならない。セットアップコスト及びテイクダウン時間を最小限にすることも重要な要素である。

パケットフィルタリングは、通過するトラフィックを制御することによって接続性を確保しつつセキュリティを与え、1つのネットワーク内、及び接続されたネットワーク間の双方において、イリーガルな通信が試みられることを防止する方法である。

従来のパケットフィルタリングのインプリメンテーションでは、固定フォーマットに従ったリストテーブルによりアクセスを特定することができる。この方法の自由度は、所定の組織のセキュリティポリシーを表すものに限定されている。また、この方法は、適用対象、即ちオブジェクトが、特定のテーブルにおいて規定されたプロトコル及びサービスの組に限定されている。この方法では、元のテーブルにおいて特定されていない異なるプロトコル若しくはサービスの導入が不可能なのである。

パケットフィルタリングを実現する他の方法では、その組織の各セキュリティポリシーについて、コンピュータオペレーティングシステムのコードを手で調整する。この方法での限界は、将来のネットワークトポロジーの変化、新たなプロトコルの使用、サービスの強化、及び将来セキュリティが脅かされる可能性に対処できる自由度がないことである。この方法では、コンピュータプログラムを適切なものに変更するために専門家による大量の作業が必要であることがシステムの欠点であって、システムのセットアップ及び維持にコストがかさむ。

更に、企業、支社、及びビジネス上のパートナーとの間の長距離の通信のセキュリティの必要性は、近年のビジネスの現実においては不可欠

なものにまで高まってきている。歴史的には、完全に私設の企業間の長距離の業務処理のためには、ネットワーク間のポイントツーポイント接続が用いられた。しかし、このようなシステムでは自由度を欠き、法外なコストがかさむことから、広く使用されるには到らなかった。インターネットのような公衆ネットワークは、長距離のインターネットワーキング用の自由度の高い低コストのソリューションを提供する。専用ラインを確立する代わりに、インターネットを媒介物として使用することにより企業間の通信が可能である。ローカルなインターネットプロバイダにひとたび接続すると、私設ネットワークはたちまち世界中のデスティ

ネーションに接続することが可能になる。

なんらかの公衆セグメントを使用する私設ネットワークは、仮想私設ネットワーク、またはバーチャルプライベートネットワーク（VPN）と呼ばれる。VPNは専用私設ネットワークと較べて極めて低コストで自由度が高い。各施設ネットワークは、ローカルインターネットプロバイダに接続するだけでよい。新たな接続を加えることも、簡単でコストがかからない。しかし、VPNの主な欠点は、セグメントのなかにセキュリティを施されていないところも含まれるため機密保護の安全性を欠くことである。インターネットへの接続は、その企業を2つの危険にさらす。それは、（1）企業内ネットワークへの不当なインターネットアクセス（ブレイクイン）、及び（2）インターネット内を通過していく企業通信の傍受及び干渉である。

インターネット上の通信に伴うセキュリティのリスクがあることによって、企業はVPNの利点を完全に享受できない。インターネット上でビジネスを実行するために（即ち、送金、クレジット情報の獲得及び認証、製品の販売及び配布）には、信頼性が高く効果的なセキュリティを施すソリューションが必要なのである。

発明の要約

従って、米国特許出願第08/168,041号の一部継続出願である本発明の目的は、コンピュータネットワーク内の情報フローを制御する、改善された、柔軟性を有し容易に変更が可能なセキュリティメソッドを提供することである。

本発明の別の目的は、ネットワーク上で内部及び外部のデスティネーションとの間を行き来する情報フローを、情報の暗号化、ソース及び/若しくはデスティネーションアドレスの変更の少なくとも一方の処理を含む形で制御することである。

本発明の更に別の目的は、システム内のノードを通過する暗号化された情報パケットを各パケット毎に検査することができるパケットフィルタによって情報フローを制御することである。

本発明の更に別の目的は、好ましくは非破壊接続有効性検査の後に、予め許可されたパケットのみを通過させることができるパケットフィルタによって情報フローを制御することである。

本発明の更に別の目的は、ノードにおける所定の、パケットを受容する（通過させる）か拒絶する（破棄する）かを定めるセキュリティ方針を実現する命令セットによって制御される、予め許可されたパケットのみを通過させる汎用パケットフィルタモジュールを提供することである。

本発明の更に別の目的は、システム管理者による変更が容易で、その変更の際してパケットフィルタ自体の特性の変更や大量のコードの書き込みが不要な、コンピュータネットワーク用セキュリティメソッドを提供することである。

本発明の更に別の目的は、改善された接続有効性チェック機構を提供することである。

本発明の更に別の目的は、何らかの暗号化手段、即ちデスティネーシ

ョンアドレスの変更、受信基準としての外部入力を受け取り、及びネットワーク通信の拒絶または変更によりパケットを変更する能力を付与することである。

本発明の更に別の目的は、インターネットのような機密保護がなされない公衆ネットワーク上でのデータフローの機密保護のための暗号化スキームを提供し、仮想私設ネットワーク（VPN）を構築できるようにすることである。

本発明の1つの側面によれば、暗号化によりネットワーク上のトランザクションの機密を保護し、異なるアドレス指定方法でさまざまなネットワーク間の相互接続をなし、また、通信のソースが許可を付与されており、ネットワーク上の通信の有効性が確認された場合にのみ、情報のパケットを通過させる方法を提供するとともに、それを達成するのに必要な情報が最小限ですみ、好ましくはフェールセーフ機能を備えたコンピュータシステムが提供される。

また、本発明の好適実施例に基づき、コンピュータネットワークにおける到着及び発信データパケットを、セキュリティルールに従って検査し選択的変更を施す方法であって、前記セキュリティルールによって検査された前記コンピュータネットワークの各アスペクトの定義を生成する過程と、前記アスペクトの定義

によって、前記アスペクトの少なくとも1つを制御する前記セキュリティルールを生成する過程と、前記セキュリティルールを、前記セキュリティルールに従って前記データパケットを検査し選択的変更を施すパケットフィルタリングモジュールの動作を制御するためのパケットフィルタリング処理言語命令セットに変換するセキュリティルール変換過程と、前記セキュリティルールに従って前記データパケットを検査し選択的変更を施すために、仮想パケットフィルタリングマシンを実現する前記パケットフィルタリングモジュールと、

前記コンピュータネットワークを接続する過程と、前記パケットフィルタモジュールが前記パケットフィルタリング処理言語命令を実行して前記仮想パケットフィルタリングマシンを操作し、前記コンピュータネットワークから、または前記コンピュータネットワークへの前記データパケットの出入りを受容若しくは拒絶し、そのようにして受容された前記データパケットを選択的変更を施すパケットフィルタリング処理言語命令実行過程とを有することを特徴とするコンピュータネットワークにおける到着及び発信データパケットを、セキュリティルールに従って検査し選択的変更を施す方法が提供される。

更に、本発明の1つのアスペクトとして、ネットワークオブジェクト、ネットワークサービス、若しくはその双方が含まれ得る。更に、オブジェクト定義はオブジェクトのアドレスを含み、また、セキュリティルール変換過程のフィルタリング処理言語命令はスクリプトの形態であって、そのスクリプトをコンパイルして、パケットフィルタリング処理言語命令実行過程において実行される命令に変換するコンパイラを更に含む。

更に、ネットワークのアスペクトを生成する過程、及びセキュリティルールを生成する過程の双方はグラフィック的に定義され、選択的変更処理は、暗号化、復号化、署名生成、及び署名確認からなる処理のグループから選択される。

また、本発明の別の好適実施例に基づき、コンピュータネットワークにおける到着及び発信データパケットを、セキュリティルールに従って検査し選択的変更を施すセキュリティシステムであって、前記セキュリティルールによって検査される前記コンピュータネットワークの各アスペクトが予め定義されており、前

記セキュリティルールが前記アスペクトによって前もって定義されており、かつパケットフィルタリング処理言語命令に変換される、該セキュリティシステムを操作する方法におい

て、前記セキュリティルールによって検査される前記コンピュータネットワークの少なくとも1つのエンティティにおいて、前記コンピュータネットワークに接続されたパケットフィルタリングモジュールを設ける過程であって、前記パケットフィルタリングモジュールが、前記コンピュータネットワークに、または前記コンピュータネットワークから出入りする前記データパケットを検査し選択的変更を施す仮想パケットフィルタリングマシンを実現する、該過程と、前記パケットフィルタモジュールが前記パケットフィルタリング処理言語命令を実行して前記仮想パケットフィルタリングマシンを操作し、前記コンピュータネットワークから、または前記コンピュータネットワークへの前記データパケットの出入りを受容若しくは拒絶し、そのようにして受容された前記データパケットを選択的変更を施すパケットフィルタリング処理言語命令実行過程とを有することを特徴とするセキュリティシステムを操作する方法が提供される。

また、本発明の更に別の好適実施例に基づき、コンピュータネットワークにおける到着及び発信データパケットを、セキュリティルールに従って検査し選択的変更を施すセキュリティシステムであって、前記セキュリティルールによって検査される前記コンピュータネットワークの各アスペクトが予め定義されており、前記セキュリティルールが前記アスペクトによって前もって定義されており、かつパケットフィルタリング処理言語命令に変換される、該セキュリティシステムを操作する方法において、前記セキュリティルールによって検査される前記コンピュータネットワークの少なくとも1つのエンティティにおいて、前記コンピュータネットワークに接続されたパケットフィルタリングモジュールを設ける過程であって、前記パケットフィルタリングモジュールが、前記コンピュータネットワークに、または前記コンピュータネットワークから

出入りする前記データパケットを検査し選択的変更を施す仮想パケットフィルタ

リングマシンをエミュレートする、該過程と、前記パケットフィルタリングモジュールが、パケットフィルタリング処理を実行するための前記パケットフィルタリング処理言語命令を読み出し、実行する過程と、前記パケットフィルタリング処理言語命令を読み出し、実行する過程において得られた結果を記憶装置に格納する過程と、

前記パケットフィルタリングモジュールが、格納された前記結果を用いて、前記パケットフィルタリング処理言語命令に基づいた前記仮想パケットフィルタリングマシンの操作を行い、前記コンピュータネットワークから、または前記コンピュータネットワークへの前記データパケットの出入りを受容若しくは拒絶し、そのようにして受容された前記データパケットを選択的変更を施す過程とを有することを特徴とするセキュリティシステムを操作する方法が提供される。

更に、本発明の別の好適実施例に基づき、コンピュータネットワークを行き来する到着及び発信データパケットを、セキュリティルールに従って検査し選択的変更を施すセキュリティシステムであって、前記セキュリティルールによって制御される前記コンピュータネットワークの各アスペクトが予め定義されており、前記セキュリティルールが前記アスペクトによって前もって定義されており、かつパケットフィルタリング処理言語命令に変換される、該セキュリティシステムにおいて、前記セキュリティルールに従って動作し、前記コンピュータネットワークに、または前記コンピュータネットワークから出入りする前記データパケットを検査し選択的変更を施す仮想パケットフィルタリングマシンを実現する、前記コンピュータネットワークに接続されたパケットフィルタリングモジュールと、前記パケットフィルタリング処理言語命令を読み出し実行する、前記パケットフィルタリングモジュールと一体化された処

理手段であって、前記パケットフィルタリングモジュールの操作を行い、前記コンピュータネットワークから、または前記コンピュータネットワークへの前記データパケットの出入りを受容若しくは拒絶し、そのようにして受容された前記データパケットを選択的変更を施す、該処理手段とを有することを特徴とするセキュリティシステムが提供される。

図面の簡単な説明

第1図は、ネットワークトポロジーの一例である。

第2図は、第1図のトポロジーのネットワークに適用された本発明のセキュリティシステムを示した図である。

第3図は、第2図のネットワーク管理部のコンピュータスクリーン上の表示を詳細に示した図である。

第4図は、グラフィカル情報をフィルタリング処理スクリプトに変換するサブシステムの流れ図である。

第5図は、本発明を利用したコンピュータネットワーク上での情報の流れを示す流れ図である。

第6図は、第5図に示すパケットフィルタの動作を示す流れ図である。

第7図は、第6図に示す仮想フィルタリングマシンの動作を示す流れ図である。

第8図は、第7図のデータ抽出方法を示す流れ図である。

第9図は、第7図の論理演算を示す流れ図である。

第10図は、第7図の比較処理を示す流れ図である。

第11図は、メモリへのリテラル値の入力方法を示す流れ図である。

第12図は、条件付き分岐操作を示す流れ図である。

第13図は、算術演算またはビット単位の演算を示す流れ図である。

第14図は、探索操作を示す流れ図である。

第15図は、記録操作を示す流れ図である。

第16図は、本発明に基づいて構築されたファイアウォールを用いている構成の一例を示す高レベルのブロック図である。

第17図は、セッション鍵の交換中に、2つのファイアウォール間で転送されるデータを示す高レベルのブロック図である。

第18図は、セッションデータの交換中に、暗号化処理を用いて他のファイアウォールへパケットを転送するファイアウォールによって実行されるプロセスを示す、高レベルの論理流れ図である。

第19図は、セッションデータの交換中に、他のファイヤウォールからの暗号化されたパケットを受け取るファイヤウォールによって実行されるプロセスを示す、高レベルの論理流れ図である。

第20図は、ベーシック鍵の交換中に、2つのファイヤウォール間で転送されるデータを示す高レベルのブロック図である。

第21図は、本発明に基づいて構築されたファイヤウォール、及びクライアントパーソナルコンピュータを用いている構成の一例を示す高レベルのブロック図である。

第22図は、セッション鍵の交換中に、クライアントパーソナルコンピュータとファイヤウォールとの間で転送されるデータを示す高レベルのブロック図である。

第23図は、ベーシック鍵の交換中に、クライアントパーソナルコンピュータとファイヤウォールとの間で転送されるデータを示す高レベルのブロック図である。

詳細な説明

到着及び発信データパケットフローの防護

第1図を参照すると、ネットワークポロジの一例が示されている。この例においては、メインサイト100が、ワークステーション102に実現されたシステム管理機構を含んでいる。このワークステーション

はネットワークに接続されており、このネットワークには、ワークステーション104、ルータ110、及びゲートウェイ106が含まれている。ルータ110は、衛星112を介してリモートサイトのゲートウェイ122に接続されている。ゲートウェイ106はルータ108を介してインターネットに接続されている。リモートサイト120はネットワークに接続されたワークステーション124を含み、このワークステーション124はゲートウェイ122を介してインターネットに接続されている。ここに示す特定の構成は一例として選択されたものに過ぎず、本発明が機能を発揮し得るネットワークの型を限定しようとするものではない。ネットワークがとり得る構成の数は実質的に無限であり、このような構

成をセットアップするための技術は当業者には周知である。本発明は実現可能な任意の形態の上で動作し得るものである。

第2図は、本発明のシステムが組み込まれた第1図のネットワークを示した図である。第2図において、第1図にも示されている構成要素は同じ符号を付して示した。図に示すように、システム管理部102は、制御モジュール210、パケットフィルタジェネレータ208、ディスプレイ206、及び記憶媒体212を含む。パケットフィルタ204は、システム管理部、第1図のワークステーション104、及びゲートウェイ106上にインストールされている。ゲートウェイ106は、このようなフィルタを2つ有し、1つはネットワークへの接続部に、他方はルータ108への接続部に設けられている。ルータ108及び110はそれぞれ、セキュリティシステムによって生成されたプログラミングスクリプトテーブルを有しているが、これは本発明の一部分を構成するものではなく、詳細については説明しない。当業者には周知のように、これらのテーブルは、ルータをプログラムするのに従来より用いられてきたテーブルに対応するものである。

パケットフィルタ204は、リモートサイト120のゲートウェイ122上にもインストールされている。パケットフィルタの1つは、衛星112とゲートウェイ122との間のコネクション上にインストールされており、第2のパケットフィルタはインターネットとゲートウェイ122との間のコネクション上にインストールされており、第3のパケットフィルタはゲートウェイとネットワークとの間のコネクション上にインストールされている。

当業者には周知のように、情報はネットワーク上をパケットの形態で流れる。第2図におけるパケットフィルタの位置は、ワークステーション、ルータ、またはゲートウェイのようなネットワーク上の特定の対象機器、即ちオブジェクトからのデータフロー、若しくはその特定のオブジェクトへのデータフローを制御できるように選択される。従って、第1図のワークステーション104のそれぞれはパケットフィルタを有し、これらのワークステーションへの情報の流れ、若しくはこれらのワークステーションからの情報の流れは個別に制御される。しかし、リモートサイト120において、パケットフィルタはゲートウェイ122と

ネットワークとの間のコネクション上に設置されており、従ってワークステーション124へのデータフロー、若しくはそのワークステーションからのデータフローを個別に制御することはできない。このような個別化された制御が必要な場合は、同様にパケットフィルタを各ワークステーション124上に設置することができる。各パケットフィルタはネットワークのセットアップ時、若しくはセキュリティシステムのインストール時にインストールされるが、追加的なパケットフィルタを後日インストールすることも可能である。このパケットフィルタは、防護の必要なワークステーション若しくはゲートウェイ等のホストデバイス上にインストールされる。

各パケットフィルタはシステム管理部102におけるパケットフィルタジェネレータ208によって生成された命令セットに基づいて動作する。これらの命令セットによって、単にパケットの通過許可若しくは不許可についてのパラメータを含むテーブルに対してパケットの内容をチェックするのではなく、そのパケットについて複雑な操作を施すことが可能となる。従って、各パケットフィルタは、パケットフィルタ自体の構造を変化させることなく、複数のセキュリティールを取り扱うとともに、極めて柔軟にセキュリティールの変更を行うことができることになる。

システム管理者は、モニタ206上に表示されるグラフィカルユーザインタフェース（GUI）を介してセキュリティールを入力する。GUIについては第3図を参照しつつ後に詳しく説明する。この情報は、パケットフィルタジェネレータ208によって処理され、その結果得られたコードはネットワーク内の適切なパケットフィルタ若しくはフィルタに転送されて、所望の機能を発揮することになる。制御モジュール210により、システム管理者がネットワークの動作を追跡することが可能となり、また記憶媒体212によりネットワーク上の操作及びネットワークへの不法な侵入の試みの記録を保持しておくことが可能となる。これによって、システム管理者が、セキュリティールがうまく機能を発揮しているか否かということや、ネットワークの動作に関する情報を完全に与えられ得

ることになる。従って、接続性を制限することなくネットワークのセキュリティを維持するための適切なネットワークの変更を、セキュリティ管理者が施すことが可能となるのである。

第3図は、第2図コンピュータスクリーン206上の表示を詳細に示した図である。スクリーンは、4つのウィンドウに分けられており、左側には2つの小さいウィンドウが、右側には2つの大きなウィンドウが

配置される形となっている。ネットワークのオブジェクト (object) 及びサービス (services) は、本発明のセキュリティメソッドにおいて規定されなければならないネットワークの2つのアスペクト (aspect) である。ウィンドウ304は、ワークステーション、ゲートウェイ、及びシステムに接続された他のコンピュータハードウェア等のネットワークオブジェクトを定めるために用いられる。いくつかのデバイスを、例えば、会社の財務部、研究開発部、及び経営者といったようにグループ化してまとめることも可能である。従って、パケットフィルタの適切な配置により、データフローの制御を、ネットワーク上の個別のコンピュータに対してのみならず、ネットワーク上のコンピュータのグループに対しても行うことが可能である。これにより、システムオペレータがネットワーク上の通信の管理に当たって自由度を大きくすることができる。例えば、会社の最高責任者 (CEO) や役員のような上層部の経営者は財務部のチーフと同様に財務部と直接通信を行うことができるが、他のグループからの通信はフィルタリングするようにすることができる。また、特定のコンピュータの組に対して、全てのグループからの電子メールを受け取ることができるが、それ以外の情報のリクエストを制限するようにすることもできる。これによってシステムオペレータが、そのネットワークの対外セキュリティと同様、内部的なセキュリティを施すことが可能となる。このオブジェクト定義は、ネットワーク上のオブジェクトのアドレスや、そのオブジェクトがネットワークの内部 (internal) または外部 (external) の何れに存在するか、パケットフィルタがそのオブジェクト上にインストールされているか否かを示す名前及びグループ、及びグラフィカルシンボルを含む。グラフィカルシンボルはルールベースマネージャ302とともに用いられる。

同様に、ネットワークサービス (service) はスクリーン上のブロック

306において定義される。これらのネットワークサービスは、login、route、syslog、及びtelnet等を含み得る。各サービスは、一般的な若しくは特別なプロパティによって定義される。一般のプロパティは、例えば、telnet用のポート番号23と等価な“dport” (デスティネーション ポート) のような、サービスを指定するコードストリングを含んでいる。発信するパケット及び到着するパケットを指定するこのコードストリングは内容が識別される。特別なプロパティはサービスの名称、そのサービスを提供するのに用いられるポートの名称、コネクションレスセッションが不使用の状態にあり得る秒数の制限時間、即ちそのセッションが終了したことが推定される前に何れかの方向に伝送されるパケットが存在しない状態にある秒数の制限時間を含む。サービス定義の他の要素には、受信した、UDPのようなコネクションレスプロトコルを用いるサービスに対する発信コネクション及びRPCサービス用のプログラム番号が含まれ得る。グラフィックシンボル及びその色は特定される。

ブロック302はルールベース (rulebase) マネージャであり、これは新たなセキュリティルールのグラフィック形式でシステム内に入力できるようにする、即ちシステム管理者を、特定のセキュリティルールを実現するため、若しくはセキュリティルールの変更のためにコードを書く必要性から解放させるものである。新たなセキュリティルールのシステムに入力するために必要な要素は4つだけである。第1要素はデータパケットのソース (source) であり、第3要素はパケットのデスティネーション (destination) である。第2要素は関連するサービス (services) のタイプであり、第4要素は実行が必要なアクション (action) である。この実行され得るアクションには、パケットがソースからデスティネーションに送られる場合であるパケットの受容 (accept)、若しくはソー

スからデスティネーションにパケットが送られない場合であるパケットの拒絶 (reject) が含まれる。パケットが拒絶された場合には、何のアクションも行われな
ないか、またはパケットがデスティネーションに届かなかったことを表す否定応

答 (NACK) が返送され得る。更に特定され得る別の要素は、その上でルールが施行されるオブジェクトを特定する、ルールのインストール先 (install on) である (第2図参照)。インストール位置が特定されない場合には、システムはパケットフィルタモジュールを、デフォルト値である通信のデスティネーション (DST) 上に設置する。しかし、このオブジェクトはデスティネーションである必要はない。例えば、インターネットからローカルホストに向かう通信は必ずゲートウェイを通過する。従って、ゲートウェイ (gateway) がソース、若しくはデスティネーションでない場合でも、ゲートウェイ上でルールを施行することが可能である。頭文字またはグラフィックシンボルを用いてデータを入力することによって、各ルールは即座に入力されてベリファイされ得、このとき書き込み、コンパイル及び新たなコードのチェックを行う必要は無い。従って、システム管理者は、セキュリティ用コンピュータプログラム作成の専門家である必要はない。サービスがシステムに既に入力されたサービスの1つである限り、システム管理機構のホストとしての役目を果たすコンピュータは、後に詳しく述べるように、入力された情報を処理して適当なパケットフィルタのための命令セットを生成する。

ブロック308はセキュリティシステムのセットアップ及び動作の概要を示すシステムステータス一覧 (system status view) である。本発明を実行する必要はない。このシステム一覧は、グラフィカルシンボルを用いてシステムの概要を表示する。この概要には、例えば、ホストアイコン、ホストネーム、ルールベースを含むファイル名であるルールベ

ースネーム、ホストにルールベースがインストールされた日付等を含まれ得る。この概要は、ホストと通信が行われたか否かということと共に、ホストによって検査され、廃棄され、及び記録されたパケット数を示すホストステータスを表示し得る。

第4図は、GUI上の情報をパケットフィルタ用に用いられるルールを含むフィルタスクリプトに変換するサブシステムを示す流れ図である。好適実施例においては、フィルタスクリプトジェネレータの出力は、オブジェクトコードにコン

パイルされ、次いで後に説明するように、パケットフィルタモジュールによってインプリメントされる。

サブシステム400はブロック402から処理を開始し、GUIからの第1ルールを含むブロック404に処理を進める。第1ルールは第3図に示すように、新たなセキュリティルールが特定されるスクリーン上の第1行である。次いで、制御はブロック406に進み、ここでルールソースネットワークオブジェクトと一致するコードが生成される。即ち、データパケットが発せられるシステムのオブジェクトの1つを表すものとしてパケットのソースがソースコートブロックに入力される。次いで、処理はブロック408に進み、ここでデータパケットがその行き先（デスティネーション）としているネットワークのオブジェクトを示すべく、デスティネーションコードブロックにコードが生成される。次いで、制御はブロック410に進み、ここで選択されたルールサービスに一致するコードが生成される。ルールサービスは以前に定義されており、システム内に格納されているか、定義されていない場合には、サービスを調整するセキュリティルールがシステムに入力されるときに定義される。次いで処理はブロック412に進み、ここでデータブロック406、408、及び410が一致しているならば、即ち、チェックの結果が真であるならば、パケットの受容若しくは拒絶を決定するコードを生成する。

受容若しくは拒絶のアクションは、セキュリティルールにおいて選択されたアクションに基づいている。次いで制御は決定ブロック414に進み、ここでシステムに追加的なルールを入力するか否かが決定される。システムにこれ以上のルールを入力しない場合には、サブシステムはブロック418で終了する。更にシステムに入力するルールが存在する場合には、処理はブロック416に進み、ここで新たなルールが入力されて処理はブロック406に戻り、プロセスが反復されてGUIの次の行に示されている次のセキュリティルールが処理される。

通信プロトコルは層を成しており、これはプロトコルスタックとも称される。ISO（国際標準化機構）は、通信プロトコル層の設定のためのフレームワークを提示する汎用モデルを定めた。このモデルは存在する通信プロトコルの機能

の理解のための基本的な参照モデルとしての役目を果たす。

I S O モデル

レイヤ	機 能	例
7	アプリケーション層	Telnet, NFS, ノベル社 NCP
6	プレゼンテーション層	XDR
5	セッション層	RPC
4	トランスポート層	TCP, ノベル社 SPX
3	ネットワーク層	IP, ノベル社 IPX
2	データリンク層 (ハードウェア インタフェース)	
1	物理層 (ハードウェア コネクション)	

通信プロトコルによって、利用する I S Oモデルにおけるレベルは異なる。ある層におけるプロトコルは、他の層において採用されているプロトコルに対する認識は持っていなくてもよい。これは、セキュリティアクションを作る重要な要素である。例えば、アプリケーション層（レベル7）が通信しようとするソースコンピュータ（レベル2，3）を識

別することができず、従って十分なセキュリティを提供し得なくともよい。

第5図は、本発明のフィルタパケットモジュールが I S Oモデル内でどのように使用されているかを示した図である。I S Oモデルの通信レイヤは、第5図の左側の符号 5 0 2 で示した部分に示されている。レベル1、即ちブロック 5 0 4 はネットワークの様々なオブジェクトと接続するための線であり得るネットワークのハードウェアコネクションである。レベル2、即ち第5図のブロック 5 0 6 は、ネットワーク上の各コンピュータ内に設置されたネットワークインタフェースハードウェアである。本発明のパケットフィルタモジュールは、このレベルと、ネットワークソフトウェアであるレベル3との間に入る。構成を完成させるため I S Oモデルの他のレベルについて簡単に述べると、レベル4、即ちブロック 5 1 0 は1つのセグメントから次のセグメントへのデータの配送に関連し、レベル5、即ちブロック 5 1 2 はネットワーク上の“セッション”の開設及び遮断を同期させる。レベル6、即ちブロック 5 1 4 はネットワーク上の様々なコンピュ

ータの間のデータの変換に関連し、レベル7、即ちブロック516はアプリケーションプログラムである。

パケットフィルタモジュールが存在するコンピュータにパケットが入ってゆくとき、レイヤ1及び2を通過した後、向きを変えて第5図の右側に示すパケットフィルタ520に進んでゆく。このパケットはブロック522において受信される。ブロック524においては、パケットはセキュリティルールと比較され、パケットがルールに一致するものであるか否かの判定がなされる。パケットがルールに一致する場合には、システム管理機構のログにその旨が記録され、不法な試行によりシステムへの入力となされる場合には、警告が発せられ得る。次いで、制御はブロック534に進み、そこでセキュリティルールの要求するところに基

づいてパケットを通過させるか否かが決定される。パケットを通過させる決定がなされた場合には、次いでパケットはレベル3、即ちブロック508に進む。パケットを通過させない決定がなされた場合には、ブロック528において否定応答（NACK）が送られ、このオプションが選択された場合には、制御はブロック530に進み、ここでパケットが破棄、即ちそのデスティネーションに向けて通過されないことになる。同様に、アプリケーションが別のデスティネーションに送るべきパケットを生成した場合には、パケットはISOモデルのレベル3、即ちブロック508からブロック522に進み、パケットを通過させる場合にレベル3、即ちブロック508でなく、レベル2、即ちブロック506に進むことを除いて、前述のものと全く同じプロセスによって処理が進められる。次にレベル2においてパケットはネットワーク上をブロック504、即ちレベル1に送られる。パケットがルールに一致しない場合には、次のルールが検索され、そのパケットがこのルールに一致するか否かが検査される。デフォルトルールは特定のソース、デスティネーション、またはサービスとは無関係に任意のパケットに一致するように設けられたルールである。このemptyルールのみがパケットを廃棄させるアクションを有している。一致する他のルールが存在しない場合、このルールが検索され、パケットを破棄させる効果をもたらす。パケットの破棄は

このような状況の下で取り得る最も安全なステップである。勿論、empty ルールを、パケットを通過させるように記述することもできる。

第6図を参照すると、第5図のブロック520が符号600を付して詳細に示されている。第6図における一般的な表示及び第7図～第10図に示されたより詳細な表示は、“パケットフィルタモジュール”なる用語の、ここで用いられている正確な定義を含んでいる。これらの図面

において示されている機能は、パケットフィルタモジュールを動作させるための最小限の機能である。第11図～第15図に示すのは、パケットフィルタモジュールに含まれ得るが、その言葉の最小限の意味においては必要ではない追加的な特徴である。

パケットフィルタモジュール“仮想マシン”として実現される。この仮想マシンは、この応用例のために、ネットワーク上のコンピュータであるホストコンピュータに存在する、第6図～第10図に示すマシンのエミュレーションとして定義され得る。

仮想マシンは、パケットを受信するブロック602から処理を開始する。このブロック602は第5図のブロック522に相当する。処理はブロック604に進み、ここでフィルタリング操作命令が命令メモリ（図示せず）から得られる。このフィルタリング操作命令は第2図に示すパケットフィルタジェネレータ208によって生成されたフィルタリング操作命令である。ブロック604でフィルタリング操作が取り込まれた後、処理は、メモリ618が初期化されるブロック606に進む。ブロック608においては、第1仮想マシン操作命令が取り込まれ、ブロック610でそれが実行される。仮想マシンは中間値を格納するのに用いられ得るスタック若しくはレジスタ618のようなメモリ機構を有している。スタック若しくはレジスタの使用方法については、以下に示すテーブルに関連してより詳細に示されている。次いで処理は決定ブロック614に進み、ここではストップ状態に到達したか否かが判定される。ストップ状態に到達していた場合は、パケットを受容するか拒絶するかの決定がなされる。この決定はブロック616において実行される。パケットが通過させられた場合は、パケットは第5

図に示すように処理される。パケットが拒絶された場合は、このパケットは破棄され、ブロック 528 及び 530 において示すように否定応答 (NACK) が送られ

てもよい。ブロック 614 においてストップ状態に到達していない場合は、次の操作命令がブロック 616 において得られ、処理はブロック 610 から反復される。

ステップ 5、即ちブロック 610 において実行され得る処理操作のタイプは、第 7 図においてより明確に示されている。第 7 図において、ブロック 610 及びブロック 614 は第 6 図に示したものと同一のものである。コネクション 613 に、並列に示されたこれらの処理操作が割り込んだ形となっている。ブロック 610 において行われるオペレーションに対しては、処理はそのようなタスクが実行される適当なブロック 702、704、若しくは 706 に進む。ブロック 702 において、データの抽出が行われ、ブロック 704 において、論理演算が行われ、ブロック 706 において比較処理が行われる。第 7 図の右側に示すように、他のブロックが仮想マシンによって実行され得る処理操作と並列に追加される。ブロック 702、704、及び 706 に示すようなサブセットは、本発明の仮想マシンにとって必要不可欠の構成要素である。これらの構成要素は第 8 図、第 9 図及び第 10 図にそれぞれ詳細に示されている。仮想マシンによって実行され得る処理操作に所望に応じて含まれる追加的な構成要素は第 11 図～第 15 図にそれぞれ示されている。

データ抽出ブロック 702 は第 8 図にその詳細が示されている。このプロセスはブロック 802 から開始され、ブロック 804 に進み、そこでパケット 806 内の特定のアドレスからデータが抽出される。このアドレスは、スタックメモリ 618、命令コードから取り込まれたものである。抽出されるデータの量もスタックメモリ、または命令コードによって決定される。抽出されたデータは、ブロック 808 においてメモリスタック 810 に入れられる。プロセスはブロック 812 で終了する。これらの図面において、制御の流れは縦方向の 1 直線上の矢印によって

示されているが、データの流れは右側の2本の矢印によって示されている。

第9図に示すのは、論理演算704の詳細である。論理演算はブロック902から開始され、制御はブロック904に進み、ここでメモリ906から第1値が取り込まれる。ブロック908において、メモリから第2値が取り込まれ、論理オペレーションはブロック910において実行される。論理演算の結果が真であった場合は、ブロック912において1がメモリ内にセットされ、論理演算の結果が偽であった場合は、ブロック914において0がメモリ906内にセットされる。プロセスはブロック916において終了する。

仮想マシンのための最後の、即ち第3の必須の処理操作は第10図にその詳細が示されている。比較処理ブロック706はブロック1002から開始され、制御は1004に進み、ここでメモリ1006から第1値が取り込まれる。制御は1008に進み、ここでメモリ1006から第2値が取り込まれる。第1値と第2値との間の比較処理がブロック1010で行われる。比較処理の結果が真であった場合には、ブロック1012においてメモリ1006内に1がセットされ、比較処理の結果が偽であった場合は、ブロック1014においてメモリ1006内に0がセットされる。プロセスはブロック1016において終了する。

以下のオペレーションは第7図には示されていないが、第7図における破線の右側に追加することができ、ブロック702、704、及び706と同様に、即ち並列に接続される。第11図に示すのはメモリへのリテラル値の入力である。このプロセスはブロック1102から開始され、制御はブロック1106に進んで、ここでリテラル値が命令コードから得られる。この値はブロック1108においてメモリ内にセットされ、プロセスはブロック1110で終了する。

条件付き分岐操作が第12図に示されている。このプロセスはブロック1202から開始され、制御はブロック1204に進み、ここで命令コードから得られた分岐条件がチェックされる。分岐条件が真であった場合は、ブロック1208においてメモリスタック1202から獲得され、ブロック1210においてチェックされる。ブロック1210における比較の結果が真であった場合には、次のステップがNにセットされ、プロセスはブロック1216で終了する。ブロック

1 2 1 0における比較の結果が偽であった場合には、プロセスはブロック1 2 1 6で終了する。分岐条件が偽であった場合には、ブロック1 2 0 4において、処理は直接ブロック1 2 1 4に進む。

算術演算またはビット単位の演算が第1 3図に示されている。このプロセスはブロック1 3 0 2から開始され、制御はブロック1 3 0 4に進み、ここでメモリ1 3 0 6から第1値が取り込まれる。第2値はブロック1 3 0 8においてメモリ1 3 0 6から取り込まれ、ブロック1 3 1 0において、算術演算またはビット単位の演算がメモリ1 3 0 6から得られた2つの値に対して施される。算術演算またはビット単位の演算の結果は、ブロック1 3 1 2においてメモリ内にセットされ、プロセスはブロック1 3 1 6で終了する。

セキュリティルールを実現する第1命令セットから、第2セキュリティルールのための第2命令セットにデータを送る必要がある場合に用いられる探索操作が、第1 4図に示されている。第6図のブロック6 0 6に示すように、新たなセキュリティルールが処理される度にメモリは初期化される。従って、第1セキュリティルールによってメモリにセットされる情報を、第2セキュリティルールは使用することができない。この問題を克服するために、各ルールに対してテーブル1～3を含む個別のメモリ1 4 1 0が与えられ、このテーブル1～3は前述の問題を克服

するために用いられ得る。テーブルへのデータの入力については第1 5図に示されており、後に説明する。探索操作は1 4 0 2から開始され、制御はブロック1 4 0 4に進み、ここでメモリ1 4 0 6から値が取り込まれる。制御はブロック1 4 0 8に進み、ここで参照したテーブルで前記値を探索することによって、メモリ1 4 1 0のテーブル1～3からデータが取り出される。制御はブロック1 4 1 2に進み、ここでブロックがテーブル内にあるか否かが判定される。この判定の結果Yesであれば、ブロック1 4 1 6においてメモリ1 4 0 6に1がセットされる。この判定の結果がNoであれば、ブロック1 4 1 4においてメモリ1 4 0 6に0がセットされる。

第1 5図を参照すると、プロセスはブロック1 5 0 2から開始され、制御は

ブロック1504に進み、ここでメモリ1506から値が取り込まれる。次いで制御はブロック1508に進み、ここでメモリ1506から取り込まれた値が、メモリ1510内のテーブル1～3内の適当な位置に配置される。制御はブロック1512に進み、ここでテーブル内への値の格納が成功したか否かに関する判定がなされる。格納が成功であった場合には、ブロック1516においてメモリ1506内に1がセットされる。格納できなかった場合には、ブロック1514においてメモリ1506内に0がセットされる。プロセスはブロック1518で終了する。

本発明のパケットフィルタリングメソッドを用いて実現されるセキュリティルールの一例として、システム内のTelnetサービスへのアクセスを許さないセキュリティルールの例を挙げて以下説明する。TelnetはTCPサービスであって、特定のTCPデスティネーションポート番号を有するものとして定義される。これは、パケットの9バイト目の位置にTCPプロトコル値6を有し、かつ、パケットの22バイ

ト目の位置に、2バイトのデータであるデスティネーションTelnetプロトコル番号23を有することによって識別される。このことは全てのTelnetリクエストパケットにおいてみられることである。

以下に示す表における第1の操作は、パケットの9バイト目の位置からIPプロトコルを取り出し、これをメモリ内におくことである。表の右側の列の“メモリ値”に示すように、この値6はメモリスタックの最上部におかれる。

次いで第2の操作が行われる。即ち上述のTCPプロトコル（ポート）番号6が、メモリ内の第2位置におかれる。第3のステップにおいて、スタックの上位の2つの層の値を比較し、結果“真”を得る。

TELNETサービス拒絶プロセス

#	パケット フィルタコード	仮想マシン操作	メモリ値 (スタック順)		
1	pushbyte [9]	抽出操作：パケットロケーション 9からIPプロトコル番号を抽出し、 メモリに入れる	6		
2	push 6	メモリへのリテラル値の入力： TCPプロトコル番号をメモリに入れる	6	6	
3	eq	比較処理：IPプロトコルと TCPプロトコルとを比較し、 結果“真”を得る	1		
4	pushs [22]	抽出操作：パケットロケーション 22からTCPプロトコル番号を 抽出し、メモリに入れる	1	23	
5	push 23	メモリへのリテラル値の入力： TELNETプロトコル番号を メモリへ入れる	1	23	23
6	eq	比較処理：TCPプロトコルと TELNETプロトコルとを比較し、 結果“真”を得る	1	1	
7	and	論理演算：TCPとTELNETの 両プロトコルが一致しているかをチェック	1		
8	btrue_drop	条件付き分岐操作：メモリ値が真 (true) ならば、拒絶状態に分岐			

次いでスタックの上位2つの層における値6は消去され、結果“真”を示す値1がスタックの最上位におかれる。第4のステップにおいて、パケット上の22バイト目の位置にあるTCPプロトコル番号23が取り出され、スタックの第2層のメモリロケーションにおかれる。第5のステップにおいてTelnetプロトコル番号のリテラル値がスタックの第3層のメモリロケーションにおかれる。第6のステップにおいて、TelnetのTCPプロトコルを含む第2、第3メモリ層のデータ値を、期待される値と比較し、結果“真”を得る。スタックの第2及び第

3の層の値は消去され、結果“真”を表す値1で置き換えられる。第7のステッ

ブにおいて、TCP及びTelnetの双方がそれぞれ一致をみたか否かを確かめるべく、論理演算が実行される。この判定はAND演算を用いてなされる。この場合、結果は“真”であり、スタックの上位2層における値が消去されて結果“真”を示す値1で置き換えられる。第8のステップにおいて、条件付き分岐操作が実行され、このときメモリ値が真である場合は、プログラムはTelnetリクエストを通過させない破棄状態に分岐する。以上より、Telnetリクエストを破棄させるルールがインプリメントされたことになる。

データフローの暗号化—導入

前に述べたように、企業間、支社間、及びビジネスパートナー間での長距離通信は、最近のビジネスには欠かせないものとなった。本発明を利用することにより、インターネットのような機密保持がなされていない公衆ネットワーク上に、仮想的な私設ネットワークであるバーチャルプライベートネットワーク（VPN）を構築することができ、これによって機密が防護され、かつ自由度の高い通信が可能となる。

発信パケットの暗号化と到着パケットの復号化、パケットへの署名、またはアドレス変換等によるパケットの変更は、パケットのフィルタモジュールによって実行される。パケットを変更するか否かの決定は、ルールベースに基づいてなされる。全てのパケットの変更、即ち暗号化、復号化、署名、及びアドレス変換は、ルールベースのコンテンツに従って選択的に実行される。例えば、暗号化が行われる場合には、ルールベース内の1つのルールが、特定のソース、デスティネーション、及びサービスの型を有するパケットに施される暗号化処理を明示的に要求しなければならない。暗号化命令はパケットフィルタリング操作記述言語に翻訳されるが、このパケットフィルタリング操作記述言語はネットワー

ク内の仮想パケットフィルタリングマシンにインストールされ、そこで実行される。

上述のように、パケットフィルタモジュールは、パケットを拒絶するか、受容するかを決定する。拒絶する場合には、パケットは破棄される。受容される場合には、パケットは様々な方法で変更され得る。あり得る変更の例を挙げると、

暗号化、復号化、及びアドレス変換等があるが、これらに限定されるものではない。以下、パケットフィルタモジュールによって選択的に実行されるパケットの暗号化及び復号化について詳細に説明する。

全体を通して用いられる表記

以下の表記は本明細書全体を通して使用されるものである。

記号	説明
g	全てのDiffie-Hellman鍵に用いられる共通ルート
p	全てのDiffie-Hellman鍵に用いられる共通モジュラス
S_{pvt}	ソース私的鍵
S_{pub}	ソース公開鍵
D_{pvt}	デスティネーション私的鍵
D_{pub}	デスティネーション公開鍵
B	ベーシック鍵
TB	短縮されたベーシック鍵
A	補助鍵
R	セッション鍵
E	セッションデータ暗号化鍵
I	セッションデータ復号化鍵
M	パケットのデータ部分
P	非暗号化パスワード
$ENC_x(Y)$	X を鍵として用いる Y の暗号化
$DCR_x(Y)$	X を鍵として用いる Y の復号化
$SIG(Y)$	Y の署名

全体を通して用いられる用語の定義

以下の定義は、本発明の処理操作を理解する助けとなるものである。

用語	定義
平テキスト (平文)	暗号化されていないテキスト
クリアテキスト	暗号化されていないテキストを表す別の用語
暗号化テキスト	暗号化されたテキスト
鍵	送り手及び特定の受け手のみが知っている情報ピース
暗号化	鍵を持っていないものがメッセージを取り扱えないように、 メッセージの平テキストを暗号化テキストに変換すること

復号化	メッセージの暗号化に用いられるものと同じ鍵を用いて暗号化テキストを平テキストに変換すること
認証	セキュリティを施されていない通信チャネルを通して誰でも容易に公開鍵を得られる信用ある第3者、即ち認証局（CA）が、受け取り手が確認できる公開鍵に対する証明を生成すること
電子署名	メッセージの内容そのものから生成され、メッセージ及び／若しくはその出所のデータの完全性を確認するために受け手が用いる情報
ネットワーク オブジェクト	ネットワークに接続され、ネットワークとの何らかの相互作用をなすハードウェア
ゲートウェイ	少なくとも2つのネットワークに接続され、それらの間にあって情報が通過するネットワークオブジェクト
ファイヤウォール またはファイヤ ウォール機能付き ネットワーク オブジェクト	通常ゲートウェイまたは終端ホストであるネットワークオブジェクトであって、コンピュータネットワーク上の到着及び発信データパケットフローの機密を保護するとともに、セキュリティルールベースに従ってデータパケットに選択的変更を施すネットワークオブジェクト

本発明に基づいて構成されたファイヤウォールを用いているネットワークの実施例を示す高レベルのブロック図が第16図に示されている。図面に示されたネットワークの例は、本発明のシステムの暗号化能力を説明するために用いられるが、これは、説明のための例として取り上げたものに過ぎない。当業者は、本発明のシステムを、他のネットワークに対しても同様に適用することができよう。ホスト1及びホスト2は共に、それぞれの私設LANに接続される。更に、ファイヤウォール1604がそのLANを通してホスト1に接続されており、同様にファイヤウォール2がそのLANを通してホスト2に接続される。両ファイヤウォールはインターネットのような公衆ネットワーク1606に接続される。また、この公衆ネットワークは機密が保護されず、信頼できないということが仮定さ

れている。認証局1（CA1）1602は、ホスト1及びファイヤウォール1に対する認証局（CA）として機能する。認証局2（CA2）1612は、ホスト2及びファイヤウォール2に対する認証局として機能する。別の実施例では、両ファイヤウォールに対して、ただ1つのCAが設けられる。各実施例において、CAの機能は全て同様である。ただ1つの違いは、ファイヤウォールが用いるどのCAが公開鍵が登録されるかという点だけである。

ホスト1及びホスト2の間の通信は機密保護されることが必要である。ホスト1からの通信は、ファイヤウォール機能を備えたネットワークオブジェクトとしての役目を果たすファイヤウォール1を介して、インターネット（即ち公衆ネットワーク）にルーティングされる。同様に、ホスト2からの通信は、同様にファイヤウォール機能を備えたネットワークオブジェクトとしての役目を果たすファイヤウォール2を介して、インターネットにルーティングされる。ホスト2への通信において、ファイヤウォール1はホスト1からホスト2に向けて送られたパケットを代

行受信し（intercept）、暗号化する。ファイヤウォール2は、ホスト2に向けて送られて送られた暗号化されたパケットを受け取り、これらのパケットを復号化する。逆方向の通信においては、ファイヤウォール2がホスト2からホスト1に向けられたパケットを暗号化する。ファイヤウォール1は暗号化されたパケットを受信し、それらを復号化してホスト1に送る。ファイヤウォール1及びファイヤウォール2によって実行される暗号化及び復号化操作は、ホスト1及びホスト2に対して透過的である。

ホスト1がホスト2とのセッションを開設した場合、ホスト1はインターネットプロトコル（IP）パケットをホスト2に送る。ファイヤウォール1はパケットを代行受信し、ホスト1及びホスト2の間の通信が暗号化、復号化、アドレス変換等何らかの形で変更されるべきか否かを判断する。この決定は、ISO層からの情報及び前のパケットから得て保持されていた情報に基づいて各セッションごとに個別に行われる。この決定プロセスは、ステートフルマルチレイヤインスペクション（SMLI）と称される。各ファイヤウォールは、前に述べたよ

うに、ネットワークオブジェクト間の到着通信データ及び発信通信データの双方をいかに取り扱うかをファイヤウォールに指示するルールベースを保持している。ホスト1及びホスト2の間の通信は暗号化されるべきか、または電子署名されるべきかが決定された後、ファイヤウォール1は一時的にパケットを留まらせ、セッション鍵交換を開始する。これについては後に詳述する。通信の暗号化または署名が施され得る前に、両サイドは共通鍵の照合をする必要がある。この共通鍵はセッション鍵Rと称され、各セッションのスタート時ごとに新たなものが生成される。機密保護されていないインターネットまたは公衆ネットワークを使用することから、ファイヤウォール1とファイヤウォール2の間の通信のみが暗号化され

るということに注意されたい。ホスト1とファイヤウォール1との間の通信及びホスト2とファイヤウォール2との間の通信は、私的であって機密保護されていることが仮定され得る私設LAN上で行われることから、暗号化されない。

セッション鍵交換—ファイヤウォール／ファイヤウォール

セッション鍵交換の間に2つのファイヤウォール間を送られるデータを示す高レベルブロック図が第17図に示されている。以下に述べるスキームは、SMLIを用いた暗号化処理のインプリメンテーションの一例に過ぎず、本発明の範囲はこれに限定されず、他の暗号化技術も用いられ得る。本発明の技術を実施するSMLIプロセスにおいて他の暗号化技術を利用し得るということは当業者には明らかであろう。例えば、他の実施例においてはSKIP標準が用いられる。データの暗号化を開始するべく、ファイヤウォール1は、初めにホスト2に対してリクエストパケットを送る。このリクエストパケットは、ファイヤウォール2でなくホスト2に向けて送られるが、これはファイヤウォール1が、ホスト2を担当するファイヤウォールのIPアドレスを認識していないからである。リクエストパケット及び応答パケットによって、ホスト1とホスト2との間の暗号化されるべき全ての通信に対して用いられる共通鍵、即ちセッション鍵Rの両サイドでの照合が可能となる。前述のように、実際に暗号化されるのは、ファイヤウォール1とファイヤウォール2との間の通信のみである。

一般に、セッション鍵Rは、デスティネーションとも称される通信を仕掛けられた側のオブジェクト（即ちファイヤウォール2）1608によって生成され、暗号化されてソースとも称される通信を仕掛けた側のオブジェクト（即ちファイヤウォール1）1604に送られる。この2つのパケット交換は、暗号化された通信が開始され得る状態になる前に

行われなければならない。暗号化セッションが確立された後、状態情報は両ファイヤウォール内に保持され、ここで、留められていた元のパケットが両ファイヤウォールを暗号化されて通過させられる。ファイヤウォール2は同じセッション鍵Rを用いてホスト2からホスト1に送られるパケットを暗号化する。

ここでセッション鍵交換について詳細に説明する。共通秘密セッション鍵Rを照合するために、本発明においては、“スタティックな”ディフィー・ヘルマン・スキーム (Diffie-Hellman scheme) を用いる。各ディフィー・ヘルマン鍵は、私的部分と公開部分とを有する。両サイドは、それぞれの私的部分及び公開部分を有する。ソース（即ちファイヤウォール1）及びデスティネーション（即ちファイヤウォール2）に対する私的鍵は、それぞれ S_{pvt} 及び D_{pvt} である。次いで、ソース及びデスティネーションの鍵の公開部分は以下のように定められる。

$$S_{pub} = g^{S_{pvt}} \pmod{p}$$

$$D_{pub} = g^{D_{pvt}} \pmod{p}$$

ソース及びデスティネーションの双方は、セッション鍵交換を有効なものとするために、互いの公開鍵を知っていなければならない。一方の側が他方の公開鍵を知らない場合、若しくは有している鍵が、古いものと認められる場合には、ベーシック鍵交換が開始される。これについては後に詳述する。両サイドは互いの公開鍵を用いて、ベーシック鍵Bを導出する。ソースは以下の計算を行う。

$$B = \{ g^{D_{pvt}} \pmod{p} \}^{S_{pvt}} \pmod{p}$$

$$= g^{S_{pvt} D_{pvt}} \pmod{p}$$

同様に、デスティネーションは以下の計算を行う。

$$B = \{ g^{S_{pvt}} \pmod{p} \}^{D_{pvt}} \pmod{p}$$

$$= g^{\text{SpvtDpvt}} \pmod{p}$$

従って、両サイドはベーシック鍵Bを共有することになる。セッション鍵Rの暗号化に際して使用するときには、ベーシック鍵Bを短縮したものが生成され、これをTBと称する。

一般に、各ファイヤウォールはディフィー・ヘルマン鍵とファイヤウォール機能を備えたネットワークオブジェクトを結びつけるテーブルを保持している。更に、ファイヤウォールは、IPアドレスとそのようなオブジェクトの1つとを結びつけるバインディング (binding) を有していなければならない。第17図に示す構成においては、ファイヤウォール1内のデータベースは、ファイヤウォール2の存在を認識するように構成されていなければならない。ファイヤウォール1は、ホスト2の暗号化ファイヤウォールがファイヤウォール2であることも認識していなければならない。ファイヤウォール1は、ファイヤウォール2の暗号化ファイヤウォールとしての役目を果たしうる可能性のあるファイヤウォールのリストを有する。各ファイヤウォールのバインディング及びネットワークオブジェクトデータベースは、個々の管理ユニットによってスタティックに管理される。

ファイヤウォール間の通信を暗号化するために、ファイヤウォールは、それ自身のベーシック私的鍵と、それが通信する必要のある、ファイヤウォール機能を備えた各ネットワークオブジェクトのベーシック公開鍵とを知っていなければならない。ビジネスパートナーのセグメントのファイヤウォールのような、外部に存在する、ファイヤウォール機能を備えたネットワークオブジェクトのベーシック公開鍵も、暗号化セッションを開設できるようにするために知っていなければならない。このような、ベーシック鍵とファイヤウォール機能を備えたネットワークオブジェクトの間のスタティックバインディングは、ファイヤウォールの内側のデータベースに予め確立されていてもよいが、後に説明するベーシッ

ク鍵交換を用いて、通信の進行中に求めることも可能である。

共通秘密ベーシック鍵Bがひとたび2つのファイヤウォールによって照合さ

れると、それは、セッションに用いられる実際の鍵、即ちセッション鍵Rを暗号化するのに用いられる。同じセッション鍵Rは、ホスト1からホスト2への、あるいはホスト2からホスト1へのデータを暗号化するために、ソース及びデスティネーションの双方によって使用される。

ソースからデスティネーションへのリクエストの要素が第17図において右向きの矢印の上に示されている。この暗号メソッドは、1または2以上の、ソースが実行可能なセッションデータの暗号化のための暗号化メソッドを含む（即ちDES、FWZ1、RC4、RC5、IDEA、トリプルDES等）。鍵メソッドは、1または2以上の、ソースが実行可能なセッション鍵Rの暗号化のための暗号化メソッドを含む（即ちDES、FWZ1、RC4、RC5、IDEA、トリプルDES等）。メッセージダイジェストメソッド（message digest method）（即ちMDメソッド）若しくはメッセージ保全メソッド（message integrity method）は、ソースが実行可能なデータ保全を実行するための1または2以上のメソッドまたはアルゴリズムを含む（即ちMD5、SHA等）。データ保全には、メッセージの一部または全ての暗号ハッシュ（cryptographic hash）の計算を伴うのが一般的である。

提案されたソース公開鍵IDは、デスティネーションが使用するとソースが推定しているベーシック公開鍵を、ID番号を介して識別する。同様に、提案されたデスティネーションベーシック公開鍵IDは、デスティネーションが使用するとソースが推定しているベーシック公開鍵を識別する。ホスト2を防護するファイヤウォール機能を備えたネットワークオブジェクトが複数存在する場合には、どのファイヤウォール機能

を備えたネットワークオブジェクトが、実際にホスト2を防護しているかをソースが認識していないため、ソースからのリクエストパケットには、多数の提案されたベーシック公開鍵が含まれる。各提案されたベーシック公開鍵は、それぞれ異なるファイヤウォール機能を備えたネットワークオブジェクトに対応している。

このリクエストにはチャレンジ鍵Cも含まれており、このチャレンジ鍵Cは

、セッション鍵交換若しくはセッションデータそのものに対して途中で攻撃を仕掛ける妨害者の裏をかくために使用される、ソース（即ちファイアウォール1）によって選択された任意のビットフィールドである。

デスティネーション（即ちファイアウォール2）は、リクエストパケットを受け取り、またその内容に基づいて、ソースに送り返される応答パケットを生成する。応答パケットの要素は、第17図における左向き矢印の上に示されている。応答パケットはリクエストパケットと類似したフォーマットを有するが、チャレンジ鍵Cのフィールドが、暗号化されたセッション鍵Rを保持するフィールドに置き換えられている点が異なっている。ここで、暗号メソッド、鍵メソッド、及びMDメソッドのそれぞれは、リクエストにあるようなオプションのリスト以外にただ1つの要素を有する。そのリストされた要素は、リクエストにおいてリストに挙げられたオプションから、デスティネーションによって選択された要素である。同様に、選択されたソースベーシック公開鍵ID及び選択されたデスティネーションベーシック公開鍵IDの双方は、リクエストで送られたオプションリストからデスティネーションによって選択された鍵IDを表すただ1つの鍵IDを含んでいる。

応答において送られるセッション鍵Rは、実際には2つの鍵を含む。1つはセッションデータ暗号化鍵（session data encryption key）E、

もう1つはセッションデータ保全鍵（session data integrity key）Iである。従って、セッション鍵Rは以下のように定義される。

$$R = E + I$$

セッション鍵は、暗号メソッド（即ち暗号化メソッド）及びMDメソッド、またはメッセージダイジェストメソッドの双方に対して生成される任意のバイトストリームである。その長さは、暗号化メソッド及びMDメソッドによって必要とされる鍵の長さの和である。それがひとたび生成されると、MDメソッド、即ちMD5によって選択され、SIG（R）によって表されるセッション鍵の署名が得られる。セッションRとSIG（R）の組み合わせは、次いで短縮されたベーシック鍵TB及びチャレンジ鍵Cの組み合わせによって形成された鍵を用いて暗号

化される。これによって、

$ENC_{(TC+C)}(R+SIG(R))$

が形成され、これは応答においてソースに送られる。

署名またはハッシュチェックサムの計算によって、ソースが受け取ったパケットが実際にベーシック鍵Bを認識しているエンティティによって形成されたという認証を、ソース側が得られる。従って応答パケットに対して強力な認証が与えられることになる。更に、ソースがチャレンジ鍵Cを選択することから、同じことを再度行うのは不可能である。

セッションデータ交換

セッションデータ交換中暗号化技術を用いてパケットを別のファイヤウォールに転送するときにファイヤウォールによって実行されるプロセスを示す高レベルの論理流れ図が第18図に示されている。図面には示されていないが、別の実施例では、セッションデータ交換を実行するためにIPSEC標準が使用される。以前に述べたように、ソース及びデスティネーションがひとたびセッション鍵Rを照合すると、暗号化され

た両ファイヤウォール間の通信が進行する。パケットの代行受信及び変更は、ISOモデルのレベル2とレベル3の間で起こる。両方向の通信とも、同じセッション鍵Rを用いて暗号化及び復号化される。送出されるパケットは、普通のTCP/IPパケットに極めて類似したものである。このパケットは、それが暗号化されているか否かを示す、あるいはその場合どの鍵が使用されるかという情報を含んでいない。この情報は、2つのファイヤウォールによって維持されている状態のなかにのみ存在する。暗号化されるトラフィックの効率及びバンド幅を増大させる役目を果たすパケットの長さの変更を行うことなく、暗号化はその場所で行われる。一般に、転送されるパケットのそれぞれは、2つの部分に分かれる。それは暗号化されないクリアテキスト部分と、暗号化される暗号化テキスト部分である。クリアテキスト部分はIPヘッダ及びTCP/UDPヘッダを含む。パケットの残りの部分はそのデータMを意味しており、クリアテキスト部分から算出される補助鍵Aとセッション鍵Rの組み合わせを用いて暗号化される。このブ

ロセスは後に詳述する。

パケット転送時にファイヤウォールによって実行される第1ステップは、パケットそれ自体のクリアテキストの内容から補助鍵Aを生成することである（ステップ1800）。使用される部分は、パケットのタイプ及びプロトコルのタイプ（即ちRPC、UDP、TCP、ICMP等）に従っており、以下のようなフィールドを含み得る。即ち、例えば、IP-ID（一部分のみ）、RPC-XID、RPC-PROGNUM、TCP-SEQ、TCP-ACK、UDP-LEN、ICMP-TYPE、ICMP-CODE、及びIP-PROTOである。次に、補助鍵A、セッションデータ保全鍵I及びパケットのデータ部分Mがバッファに配置される（ステップ1802）。次いで、MDメソッドを用いてバッファのコンテンツに署名が生成され（ステップ1804）、それは以

下のように表される。

SIG (A+I+M)

生成された署名のビットは、次いでパケットヘッダにおかれる（ステップ1806）。パケットに署名ビットを追加することは、データの保全のために重要である。パケットの長さが変更されないことから、パケットの一部分は署名ビットで上書きされなければならない。ここでパケットが暗号化される前に署名ビットがパケット内に格納されることになる。TCPパケットの場合、28ビットの署名が以下のように格納される。

- 署名の最下位8ビットが、IP-IDの最上位8ビットを置き換える。
- 1の補数演算を用いて次の16ビットがTCP-CSUMフィールドに加えられる。
- 次の4ビットが使用されないTCP-X2ニブルに格納する（これは所望に応じて行われる）。

UDPパケットに対しては、32ビットの署名が以下のように格納される。

- 署名の第116ビットが補数演算を用いてUDP-CSUMフィールドに追加され、もとのUDP-CSUMフィールドが0である場合は、同様に1の補数演算を用いてUDP-CSUMフィールドに、UDP-SPORT及びUDP

—DPORTフィールドが追加される。

●次の16ビットはUDP-LENフィールドに格納される。

署名ビットがひとたびパケット内に格納されると、パケットのデータ部分Mは暗号化され（ステップ1808）、これは以下のように表される。

$ENC_{(E+A)}(M)$

この暗号化は、セッションデータ暗号化鍵E及び補助鍵Aの組み合わせを用いた暗号メソッドで行われる。最後に、パケットは公衆ネットワーク上を転送される（ステップ1810）。

セッションデータ交換中に別のファイヤウォールからの暗号化されたパケットを受け取るときにファイヤウォールによって実行されるプロセスを示す高レベルの論理流れ図が第19図に示されている。初めに、署名を認証するために、補助鍵Aがパケットの内容から生成されなければならない（ステップ1900）。次いで、パケットのデータ部分Mが暗号メソッド及びセッションデータ暗号化鍵E及び補助鍵Aの組み合わせを用いて復号化される（ステップ1902）。これは以下のように表される。

$DCR_{(E+A)}(ENC_{(E+A)}(M))$

次に、署名ビットがパケットヘッダから抽出される（ステップ1904）。次いで、補助鍵A上の署名、セッションデータ保全鍵I及びパケットデータMがMDメソッドを用いて生成される（ステップ1906）。これは以下のように表される。

$SIG(A+I+M)$

次いで2つの署名が互いに比較される（ステップ1908）。署名が一致した場合は、署名データを上書きされたパケットに対して何らかのデータの置き換えが行われた後、パケットが送られる（ステップ1910）。署名が一致しない場合は、パケットは破棄される（ステップ1912）。

ベーシック鍵交換

前に説明したように、ファイヤウォールを備えたネットワークオブジェクトの間の通信を暗号化するために、ファイヤウォールはそれ自身の私的ベーシック

鍵及びそれが通信する必要がある各ファイヤウォールの公開ベーシック鍵を認識していなければならない。ビジネスパートナー

に属するファイヤウォールのような外部ファイヤウォールに属する公開ベーシック鍵も、暗号化されたセッションの生成のために認識されなければならない。ベーシック鍵とファイヤウォールらのスタティックな結合は、データベース内においてファイヤウォールに対して既に確立されているはずであり、若しくはベーシック鍵交換を用いて処理の進行中に成立させることができる。更に、ベーシック鍵はセキュリティを改善するために、随時変更されてもよい。本発明においては、ベーシック公開鍵がファイヤウォール内部のデータベース内に既に存在しない場合は、ベーシック公開鍵を処理進行中に得ることができる。一般に、デスティネーションのベーシック公開鍵をソースが認識していない場合、若しくはソースによって使用されるデスティネーションベーシック公開鍵が古いものであると認められた場合には、ベーシック公開鍵が得られなければならない。

何れの場合においても、ベーシック公開鍵の交換は、転送されるディフィー・ヘルマン鍵の認証を確保するために検証される。一般にメッセージの検証により、システムに対し途中で攻撃を仕掛ける妨害者の裏をかくことができる。

ベーシック鍵を交換するプロセスを以下に詳しく説明する。ベーシック鍵交換中に2つのファイヤウォール間で転送されるデータを示した高レベルのブロック図が第20図に示されている。両サイドの何れかがその通信相手 (peer) のための有効鍵を有していない場合か、古くなった鍵を有していない場合か、古くなった鍵を有していることを認識した場合には常に、認証されたベーシック鍵を送るように他の側にリクエストを行う。

ベーシック鍵交換の開始のしかたには、ベーシック公開鍵が更新若しくは交換されなければならないということをどちらの側が認識したかに

よって決まる2つの方式があり得る。典型的には、他方のベーシック鍵を有していない側がそのことを認識する。例えば、第16図を参照すると、開始側、即ちファイヤウォール1が、ファイヤウォール2に対するベーシック公開鍵を有して

いないことを認識した場合には、そこでベーシック鍵交換が開始される。別のシナリオでは、ファイヤウォール2がファイヤウォール1からのリクエストを受け取ったとき、ファイヤウォール1に対するベーシック公開鍵の古いバージョンを有していることを確認する（これはリクエストにおいて送られた、提案されたベーシック公開鍵とデータベース内のデータを比較することによって行われる）。後者のシナリオの一例が第20図に示されている。

ベーシック鍵リクエストの要素は、第20図の左向き矢印の上に示されている。ベーシックリクエストは、ソースベーシック公開鍵ID、デスティネーションベーシック公開鍵ID、暗号メソッド、鍵メソッド、及びMDメソッドを含む。これらの要素は、本明細書のセッション鍵交換—ファイヤウォール／ファイヤウォールと題されたセクションにおいて上述したものと同一のものである。ベーシック鍵交換が起こらなければならないときには、認証された鍵更新または鍵syncを他方に送る側が、リクエストにCA公開鍵IDフィールドを追加する。この新たなフィールドはどの鍵が更新を要求しているかを示し、それによってファイヤウォール2がファイヤウォール1からの応答を受け取ることを要求する認証局（CA）鍵（即ちRSA鍵）のIDである。このメッセージを受け取ったとき、ファイヤウォール1はそのベーシック公開鍵S p u bをファイヤウォール2に送るが、その前にCA公開鍵と共にCAによってなされる認証を受ける。認証はベーシック公開鍵の電子署名を生成するプロセスである。ファイヤウォール1に対しては、CA1（1602）が、ファイヤウォール1のベーシック公開鍵（第16図）を確認す

るためのCA公開鍵を生成する。ファイヤウォール2が署名の確認を行うために、CA1、即ちファイヤウォール1用の認証局（CA）からのCA公開鍵を受け取らなければならない。

ファイヤウォール1による応答の要素は、第20図の右向き矢印の上に示されている。この要素はCA公開鍵ID、ソースベーシック公開鍵S p u b及びIPアドレスまたはソースアドレスを含んでいる。更に、ソースベーシック公開鍵の署名が送られるが、これは以下のように表される。

SIG (S_{pub})

好適実施例においては、この署名の生成過程では、初めに、電子署名を生成するMDメソッドを用いて、送られるべきベーシック公開鍵から中間的署名を生成する。次いで、最終的に転送される署名を生成するべく、この中間的署名がRSA復号化関数に入力される。ソース（即ちファイヤウォール1）のIPアドレスは、そのファイヤウォール、即ちファイヤウォール1とベーシック公開鍵（S_{pub}）との間のバインド（連結）を確認するために含まれている。

ファイヤウォール1からの認証を受け取ったとき、ファイヤウォール2はCA公開鍵を用いてそれを確認することができる。正しいと確認された場合には、ファイヤウォール2は、そのデータベースをファイヤウォール1の新たなベーシック公開鍵に更新する。ここで、セッション鍵交換が完了し、セッションデータの通信が行われ得ることになる。

ここで、ベーシック公開鍵が、各ファイヤウォールとそのCAとの間を機密保持された通信チャネルを介して通信されることに注意されたい。1または2以上のCAが存在する場合には、1つのCAの公開鍵は他のCAに妨げられることなく送られる。このメッセージは、CA公開鍵の以前の値を用いて署名されるか、あるいは新たに得られたCA公開鍵が

FAXまたは電話等のマニュアルな手段を用いて確認され得る。

セッション鍵交換—クライアント／ファイヤウォール

以前に説明したように、ビジネス上、企業ネットワークへの外部からのアクセスの必要性が高まってきている。会社のLANまたはWAN環境から物理的的外部で働いているが、それに接続する必要がある社員の数も増加している。本発明により、システムの外部ユーザを確認することが可能となり、外部ユーザ若しくはクライアントとホストシステムとの間の暗号化された通信が可能となる。

本発明に基づいて構築されたファイヤウォール及びクライアントパーソナルコンピュータを備えた構成の例を示す高レベルのブロック図が第21図に示されている。パーソナルコンピュータ（PC）2100は、説明の便宜上ここではリソースと称され、クライアントまたは外部ユーザがLANに接続されたホスト21

04のログインするのに使用される。このPCは公衆ネットワーク1606に接続されており、ファイヤウォール2102を介して、説明の便宜上サーバまたはデスティネーションと称されるホストと通信を行う。PCとホストとの間の全ての通信は、ファイヤウォールを通してなされる。このPCはホストにログインし、それとファイヤウォールとの間の暗号化通信を実行するのに必要な機能を発揮するべく適切にプログラムがなされている。第16図に示されている構成と同様に、第21図の構成においても、暗号化通信はPCとファイヤウォールとの間でのみ行われる。ホストに対しては、ファイヤウォールは透過的であり、データがPCから直接入ってくるものとみなすことができる。

ファイヤウォールに対するクライアント用のセッションデータ交換プロセスは、ファイヤウォールに対するファイヤウォールのそれに類似している。しかし、セッション鍵交換及びベーシック鍵交換プロセスに異

なる点がある。ファイヤウォールーファイヤウォールセッション鍵交換においては、各セッションが異なるセッション鍵を受信していた。セッションは、2つの特定のネットワークオブジェクト間のコネクションであるのみならず、同じネットワークオブジェクト間の異なるサービスの間のコネクションを含み得る。これに対し、クライアントはホストとのセッション及びクライアントがリクエストした動作若しくはサービスがいかなるものであれ、同じ鍵を用いてセッションが暗号化されるときに、クライアントとホストの間の全ての通信を初期化する。更に、ファイヤウォール間の通信においては、両サイドが互いの認証公開鍵を有していた。クライアントとファイヤウォール間の通信においては、このことはクライアントに対してのみ当てはまり、サーバはクライアントが送るネーム/パスワードのデータ対を用いてクライアントを識別する。

セッション鍵交換中のクライアントパーソナルコンピュータとファイヤウォール間のデータ転送を示す高レベルブロック図が、第22図に示されている。クライアントによるリクエストにおいて送られた要素は、右向きの矢印の上に示されている。この要素は、名前(name)、暗号メソッド、鍵メソッド、MDメソッド、パスワードメソッド、ソースベーシック公開鍵S p u b、提案されたデスティ

ネーションベーシック公開鍵ID、チャレンジ鍵C、暗号化されたパスワード及び署名を含んでいる。名前は、クライアントを現在用いているユーザを識別するのに用いられる。暗号メソッド、鍵メソッド及びMDメソッドについては以前に説明した。パスワードメソッドは、パスワードの暗号化に際してどの暗号メソッドを用いるかを示す。暗号化されたパスワードは以下のように表され得る。

$ENC_{(TB+C)}(P)$

ソースベーシック公開鍵S p u bは、ファイヤウォールがユーザのリス

ト及びそれに関連するベーシック公開鍵を保持していない時は常に送られる。送られるデータは、本明細書のベーシック鍵交換—ファイヤウォール／ファイヤウォールなる表題のセクションで説明したように、ファイヤウォール1からファイヤウォール2（第20図）に送られるデータに類似したものである。デスティネーションベーシック公開鍵IDは、本明細書のセッション鍵交換—ファイヤウォール／ファイヤウォールなる表題のセクションで説明したのと同じのものである。

署名はデスティネーション、即ち受け取り側に対してメッセージが変更されなかったことを確認する役目を果たす。この署名は、第22図においてTで表されているリクエストまたはメッセージの全内容のうち、署名フィールドを除く全内容を取り出し、Tと暗号化されていないパスワード及び短縮されたベーシック公開鍵TBを結びつけることによって生成され、以下のように表される。

$SIG(T+P+TB)$

この署名はリクエストに追加され、次いでこのリクエストはファイヤウォールに送られる。

リクエストが受け取られた後、ファイヤウォールは、クライアントのソースベーシック公開鍵S p u bを認識する。ここで、ベーシック鍵B及び短縮されたベーシック鍵TBの生成が可能となる。次いで、パスワードPの暗号化が可能となる。ひとたびPが認識されると、ファイヤウォールはリクエスト内の署名を確認することができる。次に、ファイヤウォールはクライアントからのリクエストにおいて送られたチャレンジ鍵C及び短縮されたベーシック鍵TBを用いて、任

意のセッション鍵R及びRの署名を生成してそれを暗号化する。これを式で表すと以下ようになる。

$$ENC_{(TB+C)}(R+SIG(R))$$

次いで、署名が、第22図においてUで示されたリクエストの内容と共に、短縮されたベーシック鍵TBから生成される。これを式で表すと以下ようになる。

$$SIG(U+TB)$$

次いでファイヤウォールは、その要素が第22図の左向き矢印の上に示されている応答を生成する。この応答はデスティネーションベーシック公開鍵ID、暗号メソッド、鍵メソッド及びMDメソッド、暗号化されたセッション鍵及び署名を含む。

セッション鍵がクライアントとファイヤウォールの双方によってひとたび認識されると、ファイヤウォールを介してのPCとホストの間の通信セッションを進めることができるようになり、PCとファイヤウォールとの間の暗号化通信はホストに対して透過的となる。鍵交換の数を減らすために、セッション鍵Rは同じファイヤウォールを通る全ての暗号化コネクションに対して用いられる。所定の時間の経過後、即ち数分間の経過後、セッション鍵Rは破棄される。

ベーシック鍵交換—クライアント／ファイヤウォール

ファイヤウォールとファイヤウォールとの間の通信とは異なり、認証された鍵の交換は、ファイヤウォールのベーシック公開鍵でクライアントを更新するためにのみ必要である。ベーシック鍵交換開始には2つの場合があり得る。その1つはクライアントがファイヤウォールベーシック公開鍵を有していない場合、もう1つはファイヤウォールが、リクエストに際してクライアントによって使用されるベーシック公開鍵が古くなっていることを確認した場合である。

このプロセスは、以前にベーシック鍵交換—ファイヤウォール／ファイヤウォールなる表題のセクションで説明したようなベーシック鍵交換に類似したものである。しかし、以下のような相違点がある。クライア

ントがファイヤウォールのベーシック公開鍵を有していないことを認識した場合

、リクエストにおけるデスティネーションベーシック公開鍵IDフィールドの代わりにCA公開鍵IDフィールドを用いる。このことは第23図の右向き矢印の上に示されている。第23図は、ベーシック鍵交換中のクライアントパーソナルコンピュータとファイヤウォールとの間のデータ転送を示す高レベルのブロック図である。この鍵IDは、ファイヤウォールからの応答を受け取ることを要求しているクライアントによる認証局(CA)鍵(即ちRSA鍵)のIDである。

ファイヤウォールは、クライアントからリクエストを受け取ったとき、リクエストを元に、クライアントがファイヤウォールのベーシック公開鍵をリクエストしているのか、リクエストにおける鍵IDがファイヤウォールのベーシック公開鍵と一致していないか否かを判定する。ファイヤウォールの応答の要素は、図面の左向き矢印の上に示されている。この応答は、元の提案されたデスティネーションベーシック公開鍵ID、CA公開鍵ID、デスティネーションベーシック公開鍵D_{pub}、デスティネーションのアドレス、及び署名を有している。元のデスティネーションベーシック公開鍵は、デスティネーションからの場合と同様に取り出される。デスティネーションベーシック公開鍵の署名が送られるが、この署名を式で表すと以下のようになる。

$SIG(D_{pub})$

好適実施例において、この署名の生成は、電子署名を生成するMDメソッドを用いて、送られたベーシック公開鍵から中間的署名を生成することによってなされる。次いで、この中間的署名は、最終的に転送される署名を生成するべくRSA復号化機構に入力される。デスティネーション(即ちファイヤウォール)のIPアドレスは、ファイヤウォールとベーシック公開鍵D_{pub}との間のバインドを確認するために含まれて

いる。

ファイヤウォールからの認証のためのデータを受け取ったとき、クライアントはCA公開鍵を用いてそれを認証することができる。それが正しいと認証された場合には、クライアントはそのデータベースをファイヤウォールの新たな公開鍵で更新する。

ファイヤウォールの応答を受け取った後、クライアントはメッセージを送り返して認証を完了する。メッセージの要素は、第23図の下側の右向き矢印の上に表示されている。このメッセージには、暗号化されたパスワード及び署名が含まれている。応答がひとたび受け取られると、クライアントはベーシック鍵B及び短縮されたベーシック鍵TBを生成することができる。次いでクライアントはパスワードPを暗号化し、これを式で表すと以下のようになる。

$$ENC_{(TB+c)}(P)$$

この署名は第22図における右向き矢印の上に表示されたような、ファイヤウォールに送られる元のリクエスト（Tとして表されている）と、クリアテキストパスワードP、及び短縮されたベーシックキーTBの組み合わせを元にして、MDメソッドを用いて生成され、これを式で表すと以下のようになる。

$$SIG(T+P+TB)$$

次いで、暗号化されたパスワード及び署名がファイヤウォールに送られる。こうしてセッションキー交換が完了し、セッションデータ通信を開始できるようになる。

本発明のいくつかの実施例について以上説明してきたが、その様々な変更、改良、及び別の形態の応用が可能であることは明らかであろう。

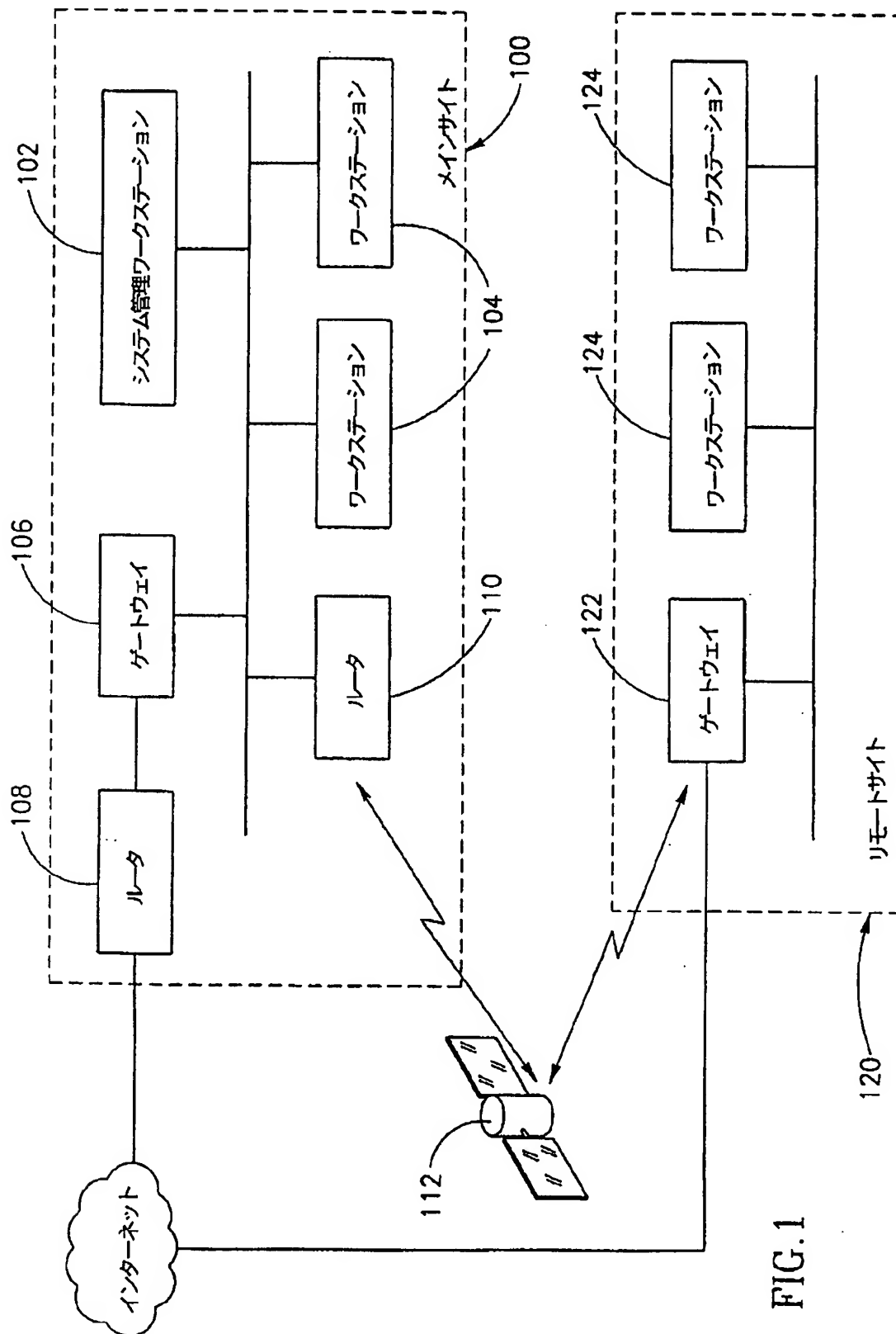


FIG.1

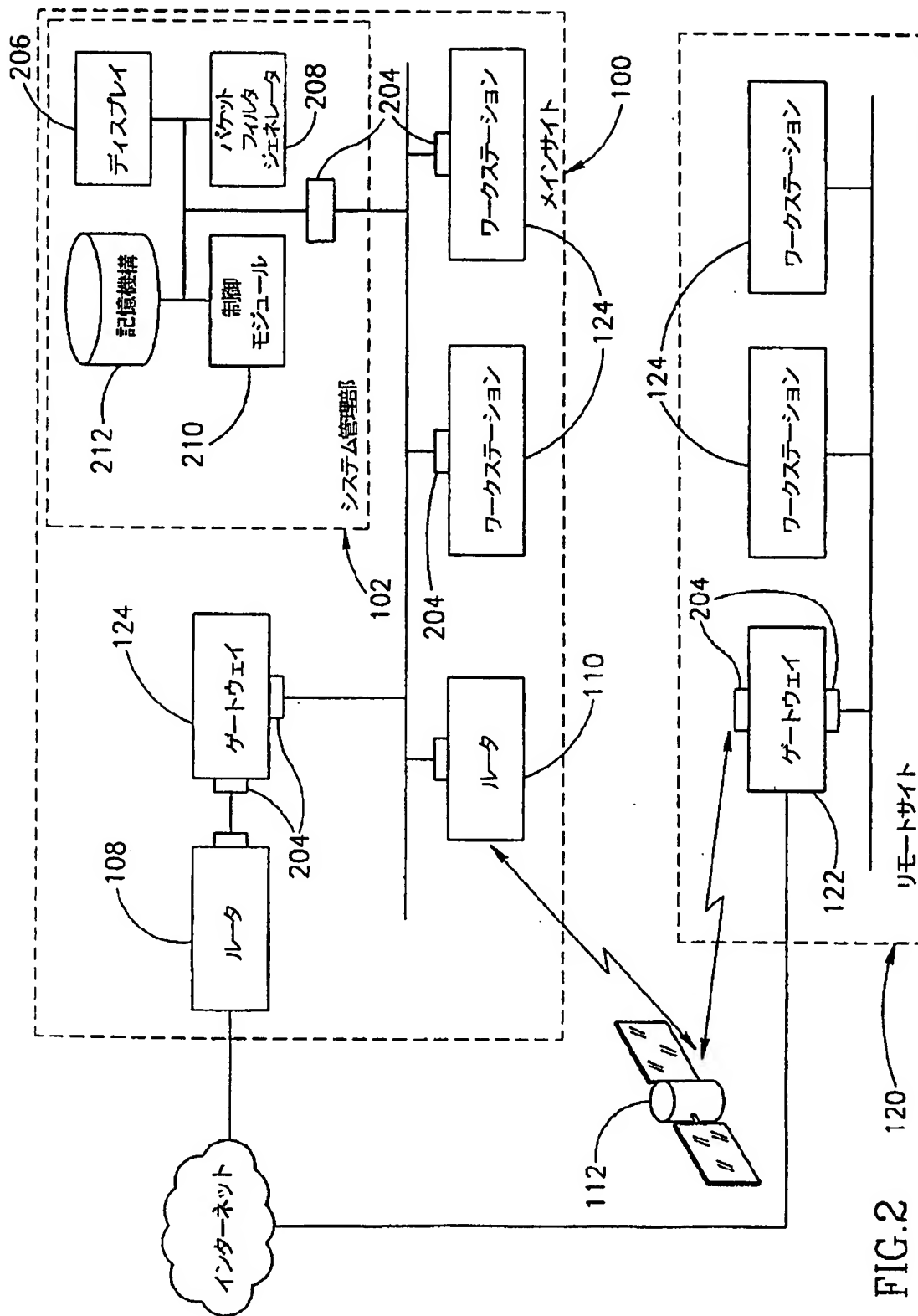


FIG.2

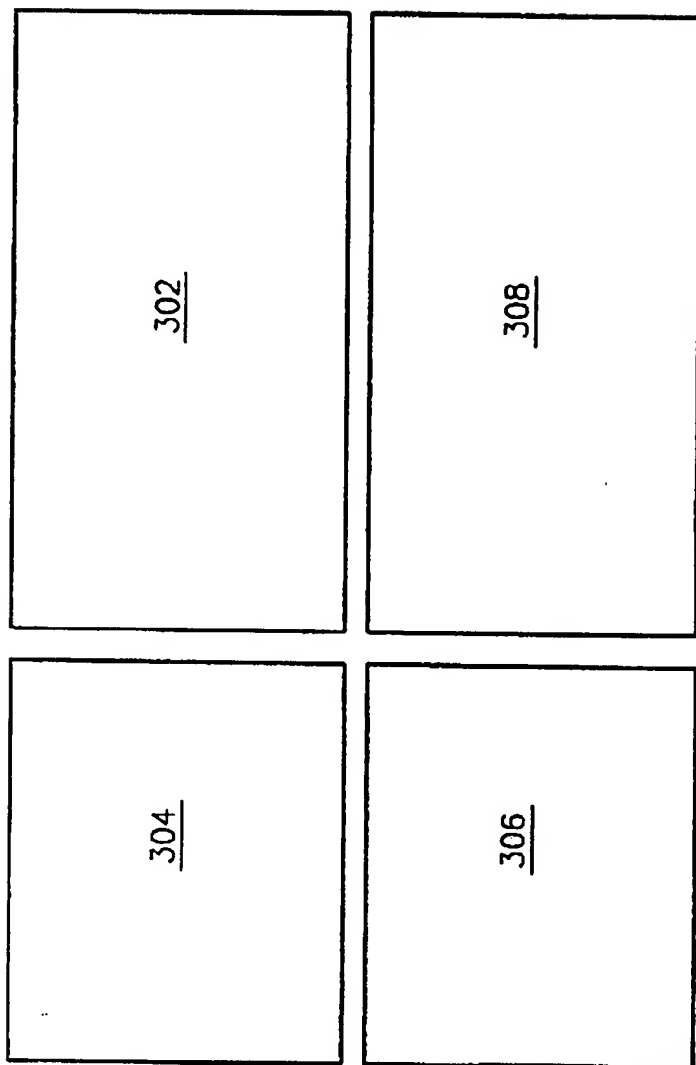


FIG.3/1

304

NETWORK OBJECT MANAGER

VIEW BY TYPES:

INTERNAL

EXTERNAL

☒ HOST

☒ GATEWAY

☒ NET

☒ DOMAIN

☒ ROUTER

☒ GROUP

BRM.CO.IL

CEO

CFO

FINANCE

INTERNAL

MAILSERVERS

TRUSTEDPARTIES

DYLAN

LOCALNET

.....

DELETE SELECTED OBJECTS

CREATE NEW OBJECTS

MAILSERVERS

FIG.3/2

SERVICES MANAGER

VIEW BY TYPES:

☒ TCP

☒ RPC

☒ GROUP

☒ UDP

☒ OTHER

X11

AUTH_TELNET

BLFF

DAYTIME

DISCARD

ECHO

EXEC

FINGER

FTP

.....

DELETE SELECTED OBJECTS

.....

▲

▼

FIG.3/3

RULE BASE EDITOR : CORPORATE

FILE
RULE
FILTER
ROUTER
UTILITES
PROPERTIES
TUTORIAL

WINDOWS: ☒ NETWORK OBJECTS ☒ SERVICES ☒ SYSTEM VIEW ☐ LOG VIEWER

NO.	SOURCE	DESTINATION	SERVICES	ACTION	TRACK	INSTALL ON
1	ANY ⊖	MAILSERVERS ⊖	SMTP	ACCEPT ⊖		GATEWAYS H-GW-H
2	<input type="checkbox"/> CEO <input type="checkbox"/> CFO	FINANCE ⊖	ANY ⊖	DROP STOP	ALERT (M)	GATEWAYS H-GW-H
3	TRUSTEDPARTIES ⊖	INTERNAL ⊖	TALK RSTAT TELNET	ACCEPT ⊖		DST ⊖
4	INTERNAL ⊖	ANY ⊖	ANY ⊖	ACCEPT ⊖	ALERT (M)	GATEWAYS H-GW-H
5	ANY ⊖	INTERNAL ⊖	FINANCE ⊖	REJECT STOP	MAIL ⊖	DST ⊖

⊖ ⊖

RULE BASE SAVED TO 'FW/USERS/MARLUS/CORPORATE.W'

FIG.3 /4


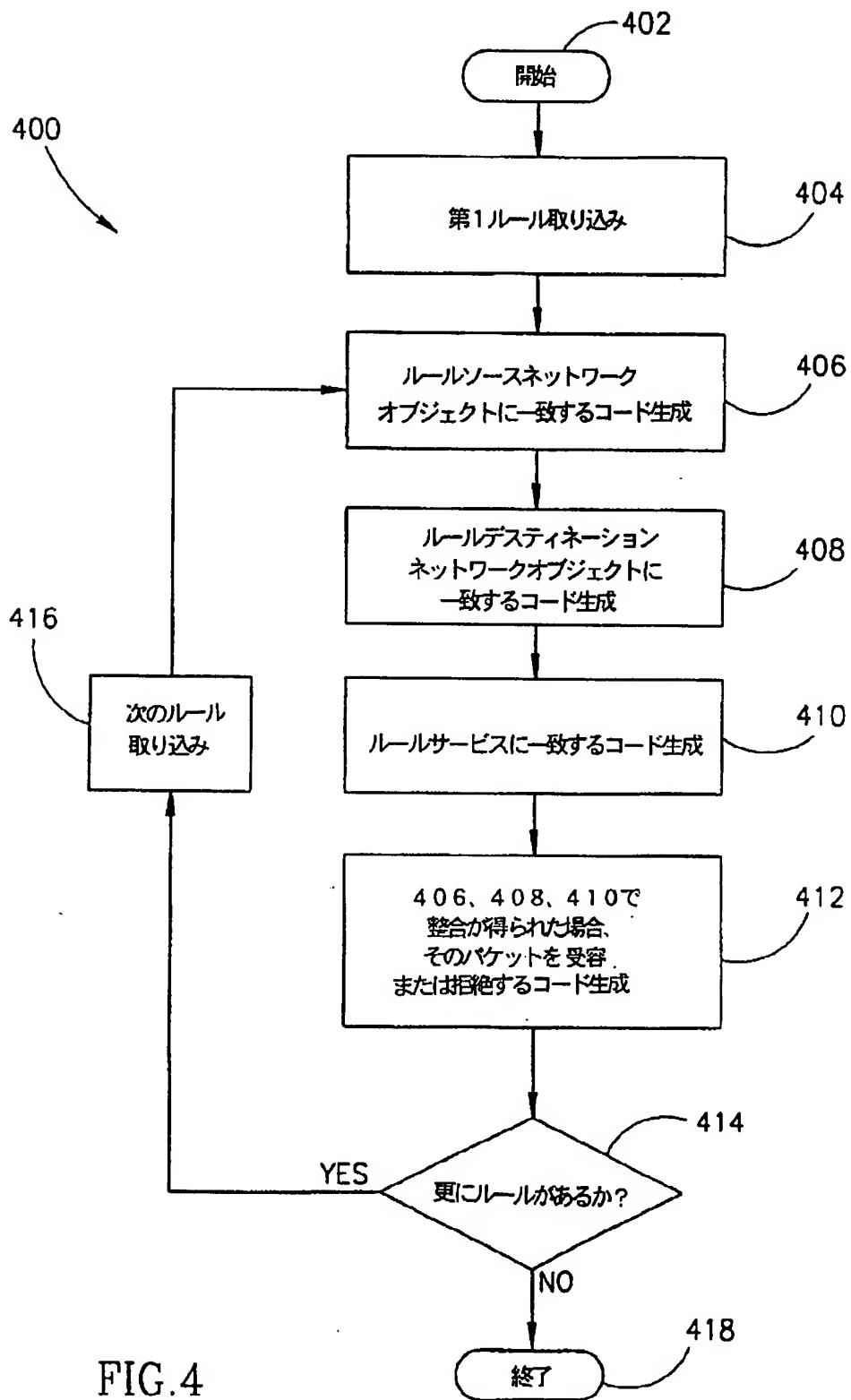
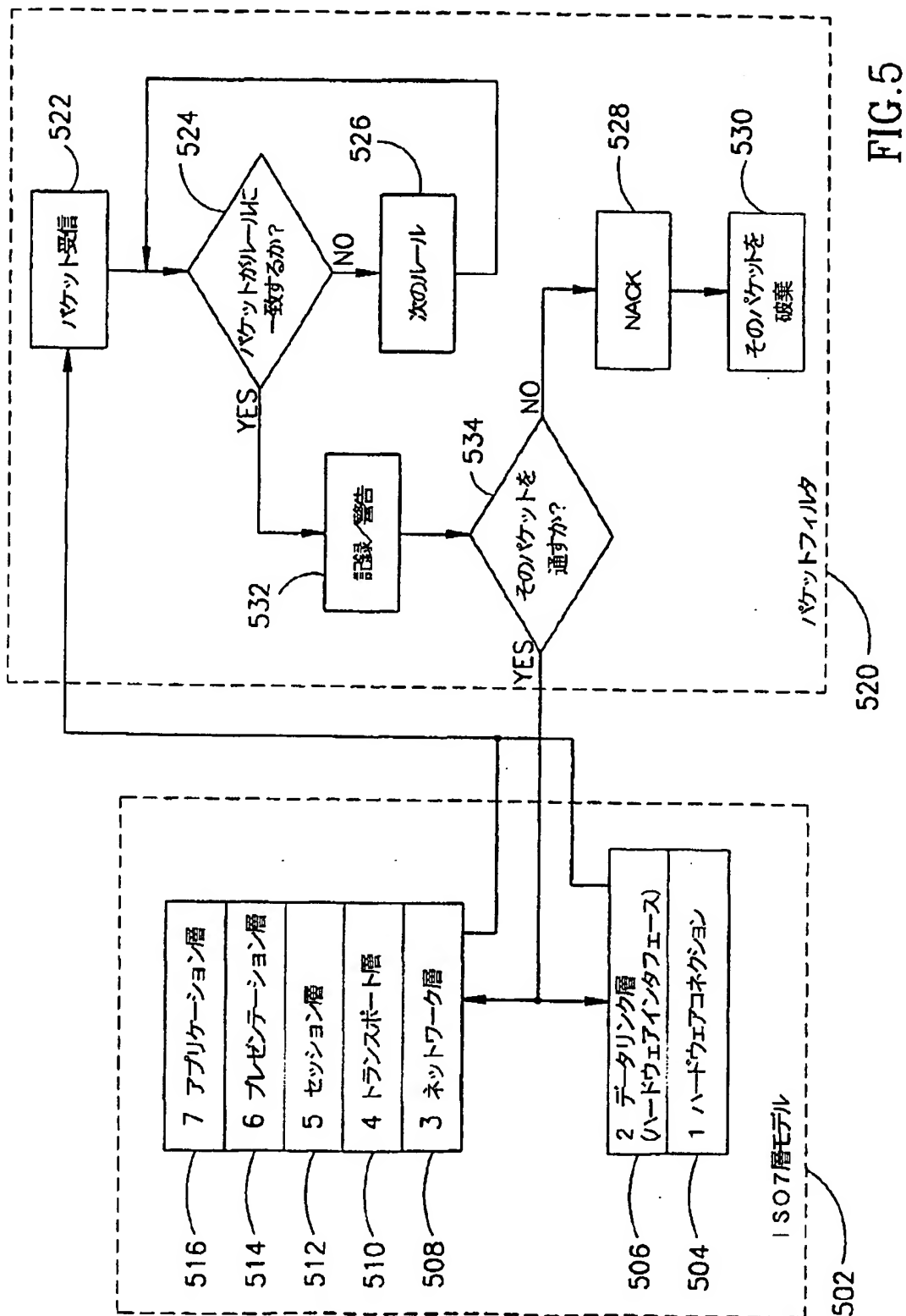
SYSTEM STATUS VIEW			
UPDATE	SHOW	INSTALL	LAST UPDATE : 16 : 21 : 42 NOW : 16 : 26 : 16
UPDATE INTERNAL (SEC):		01	120
		SELECT ALL	CLEAR SELECTIONS
<div>  <p>MONK DEFAULT</p> <p>✓ 1808-12 ● 0 ✗ 21</p> </div>			
10 DEC 93 13 : 02 : 35 10 DEC 93 16 : 20 : 53			

FIG.3/5 308

【図4】



【図5】



【図6】

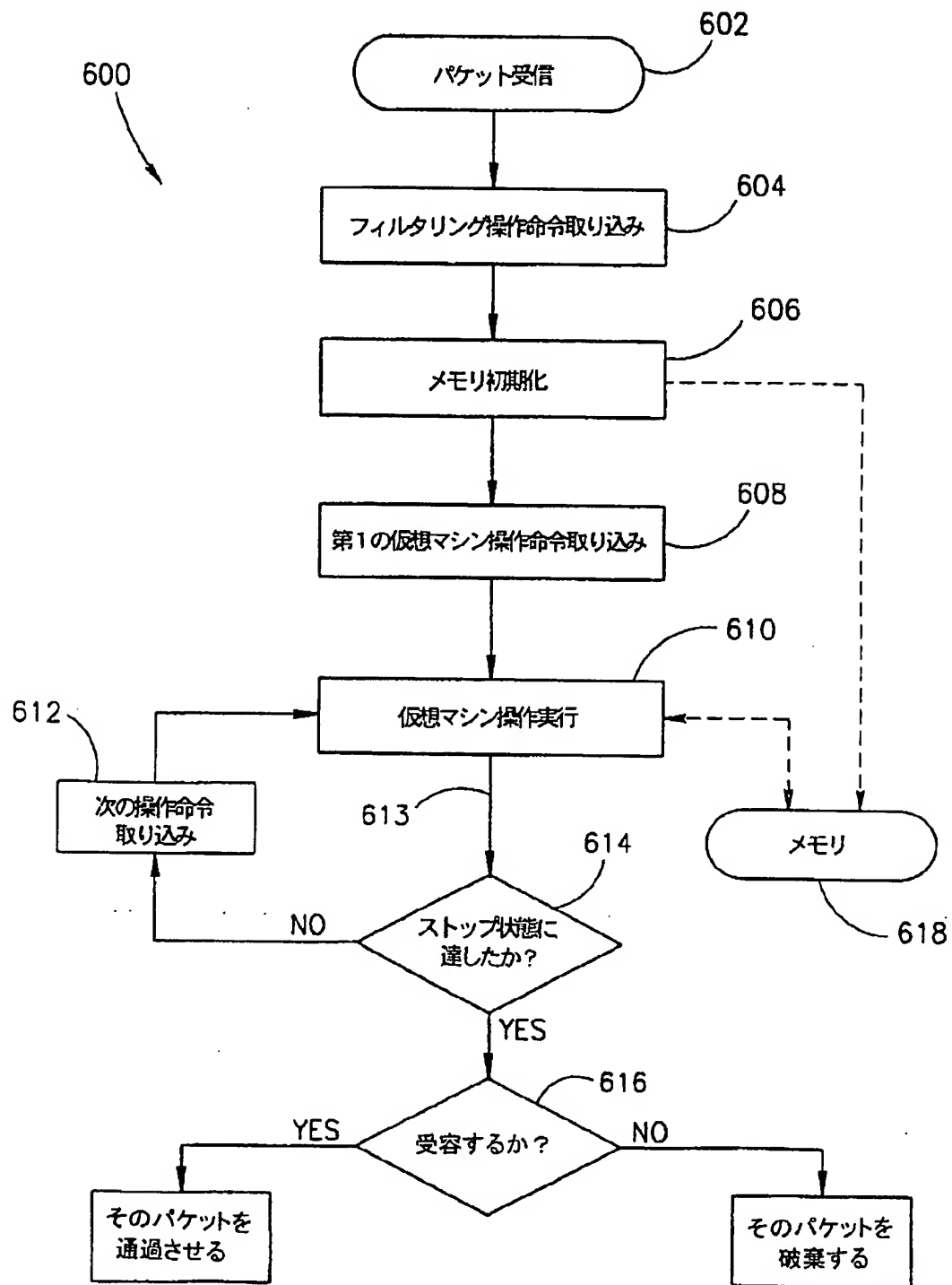
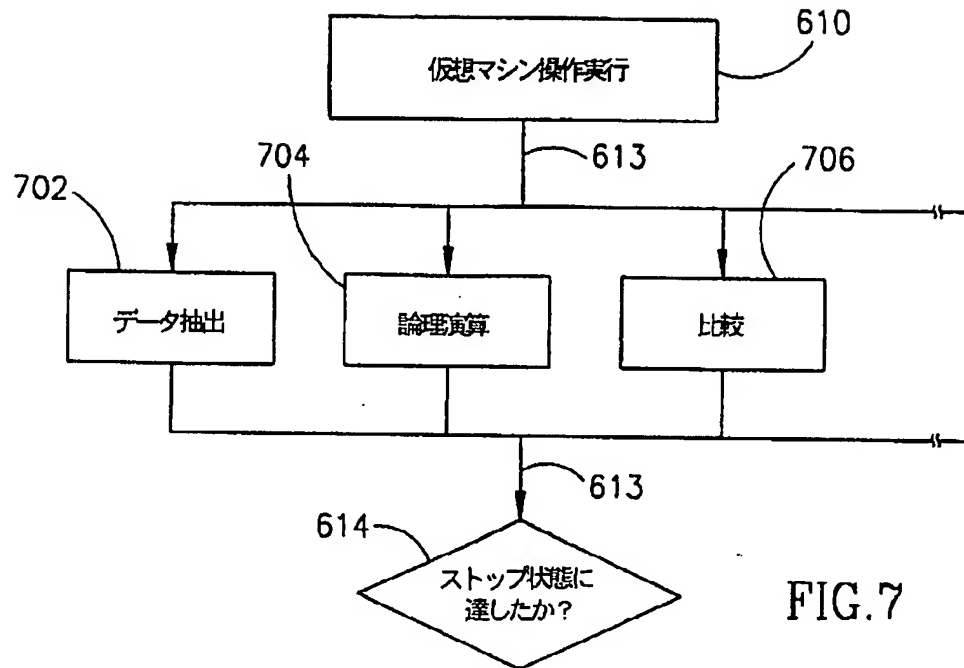


FIG.6

【図7】



【図8】

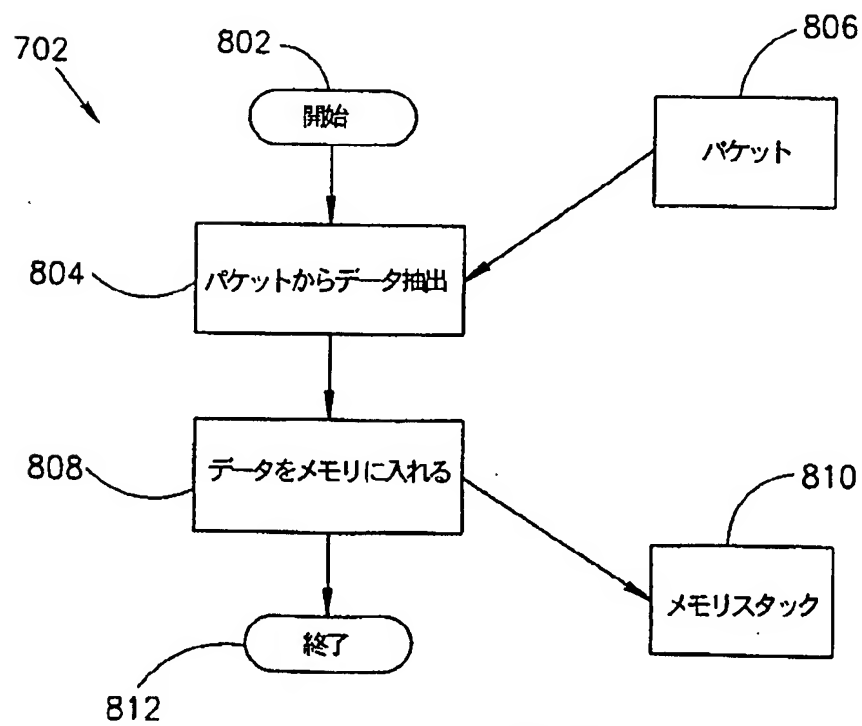


FIG.8

【図9】

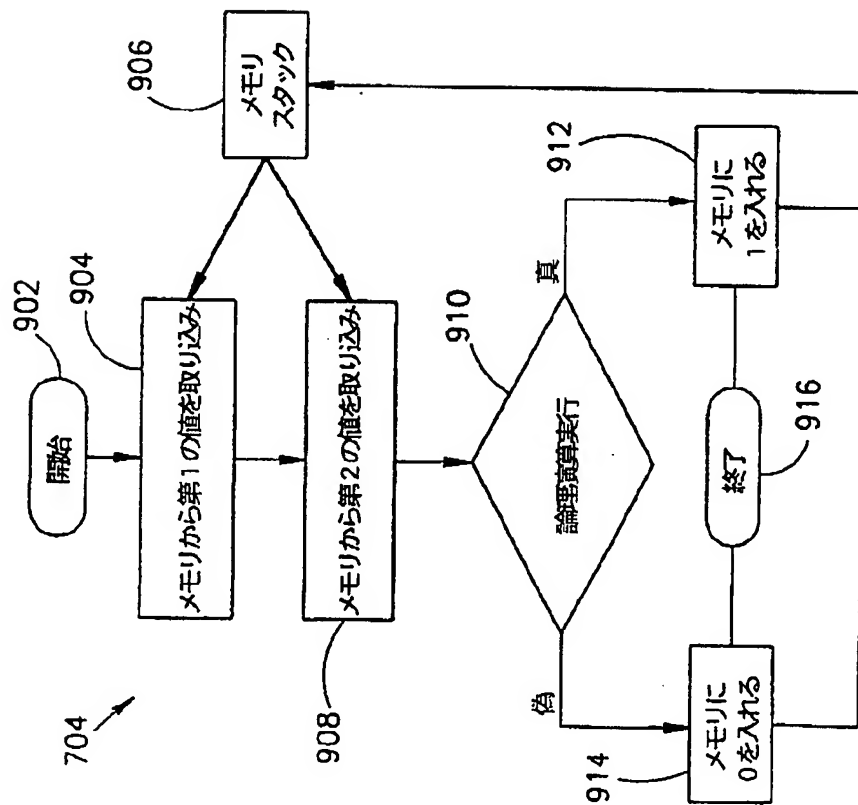


FIG.9

【図10】

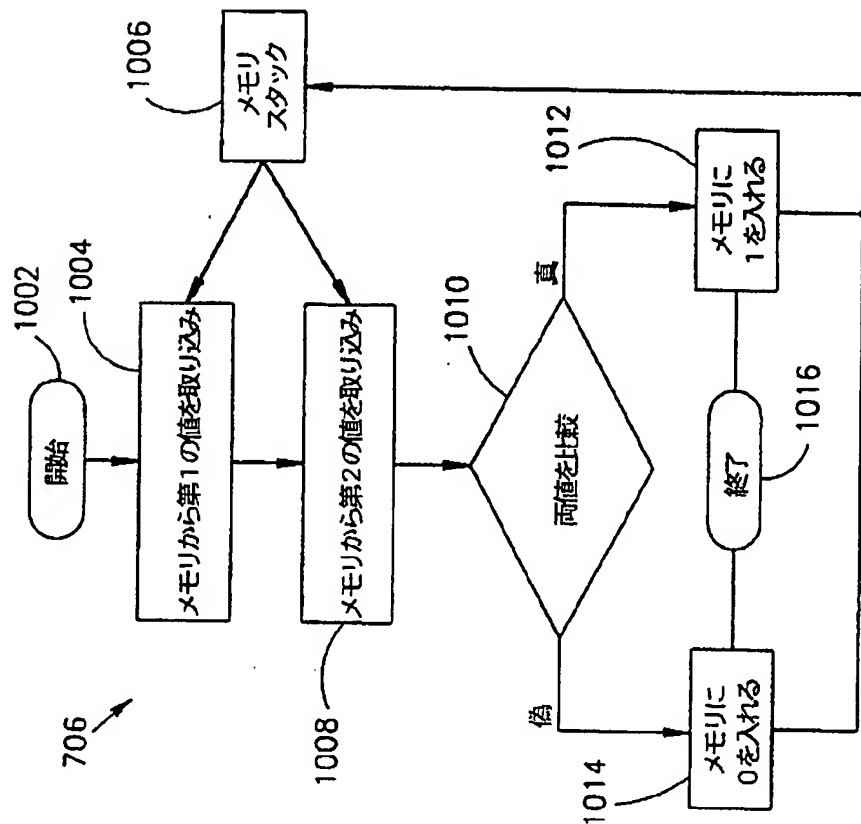


FIG.10

【図11】

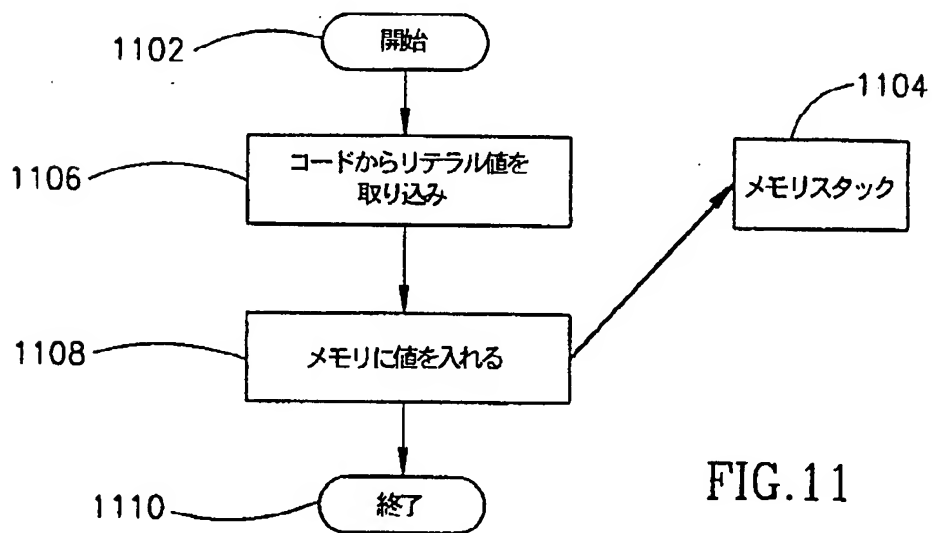


FIG.11

【図12】

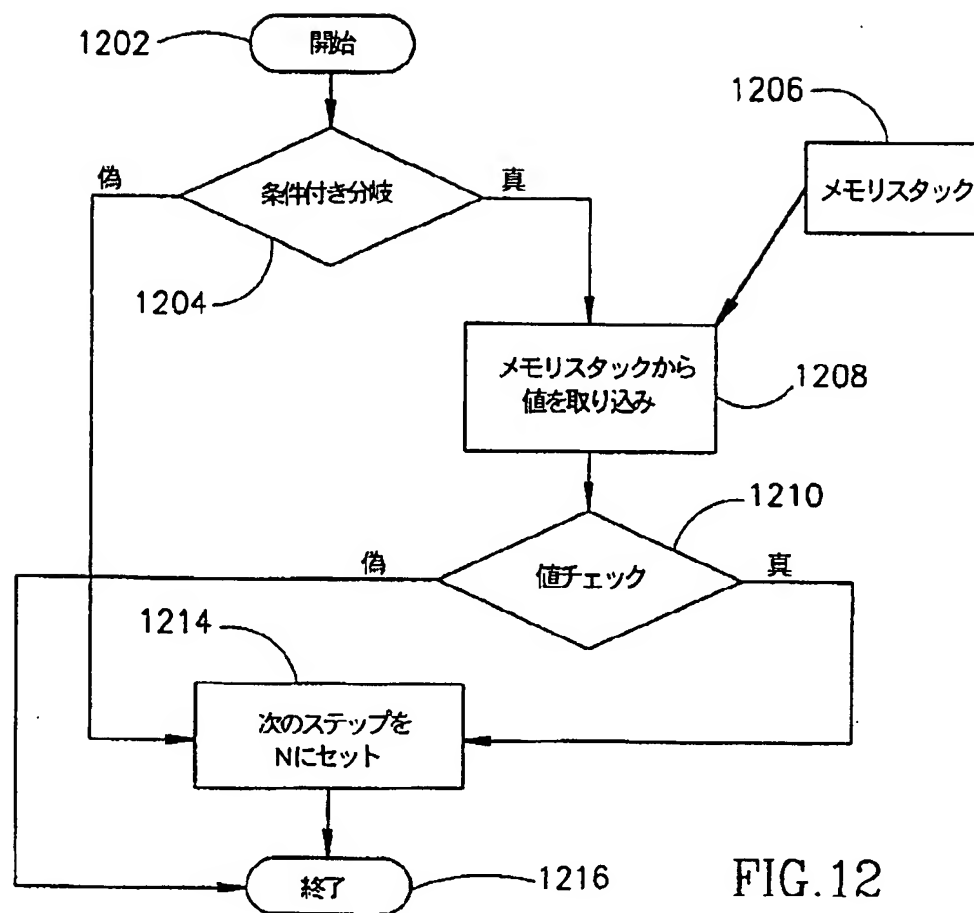


FIG.12

【図13】

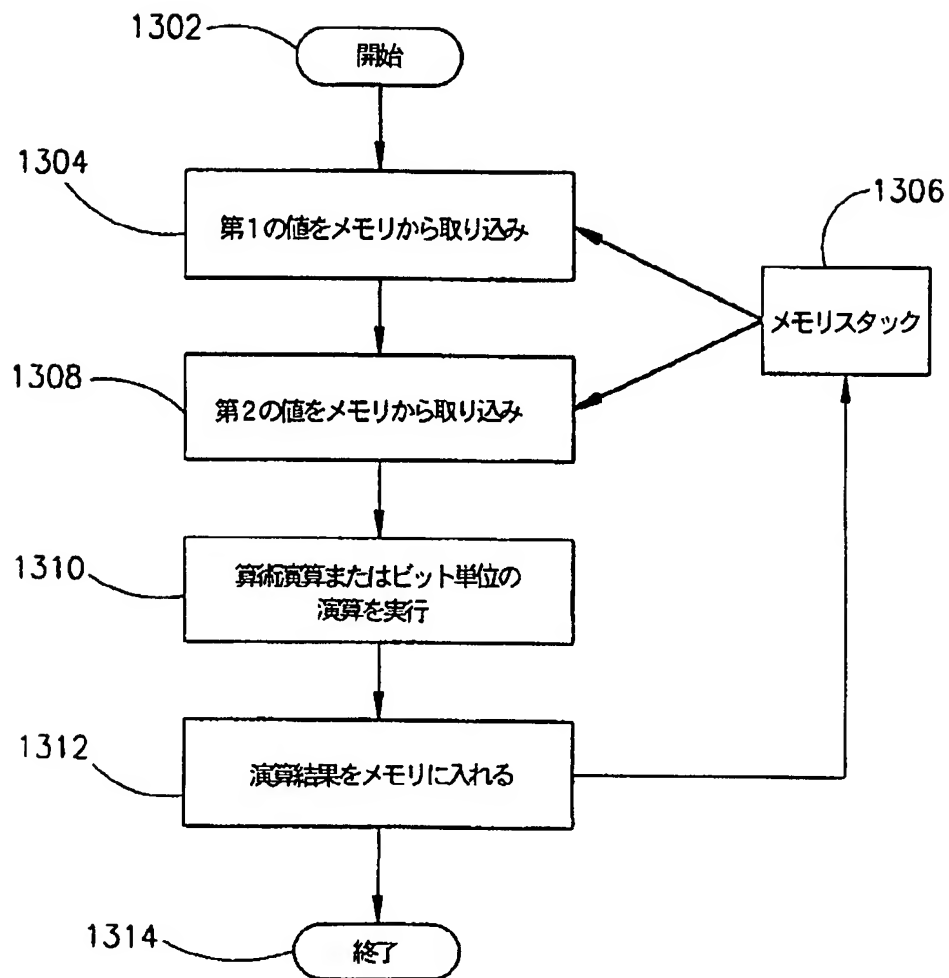


FIG.13

【図14】

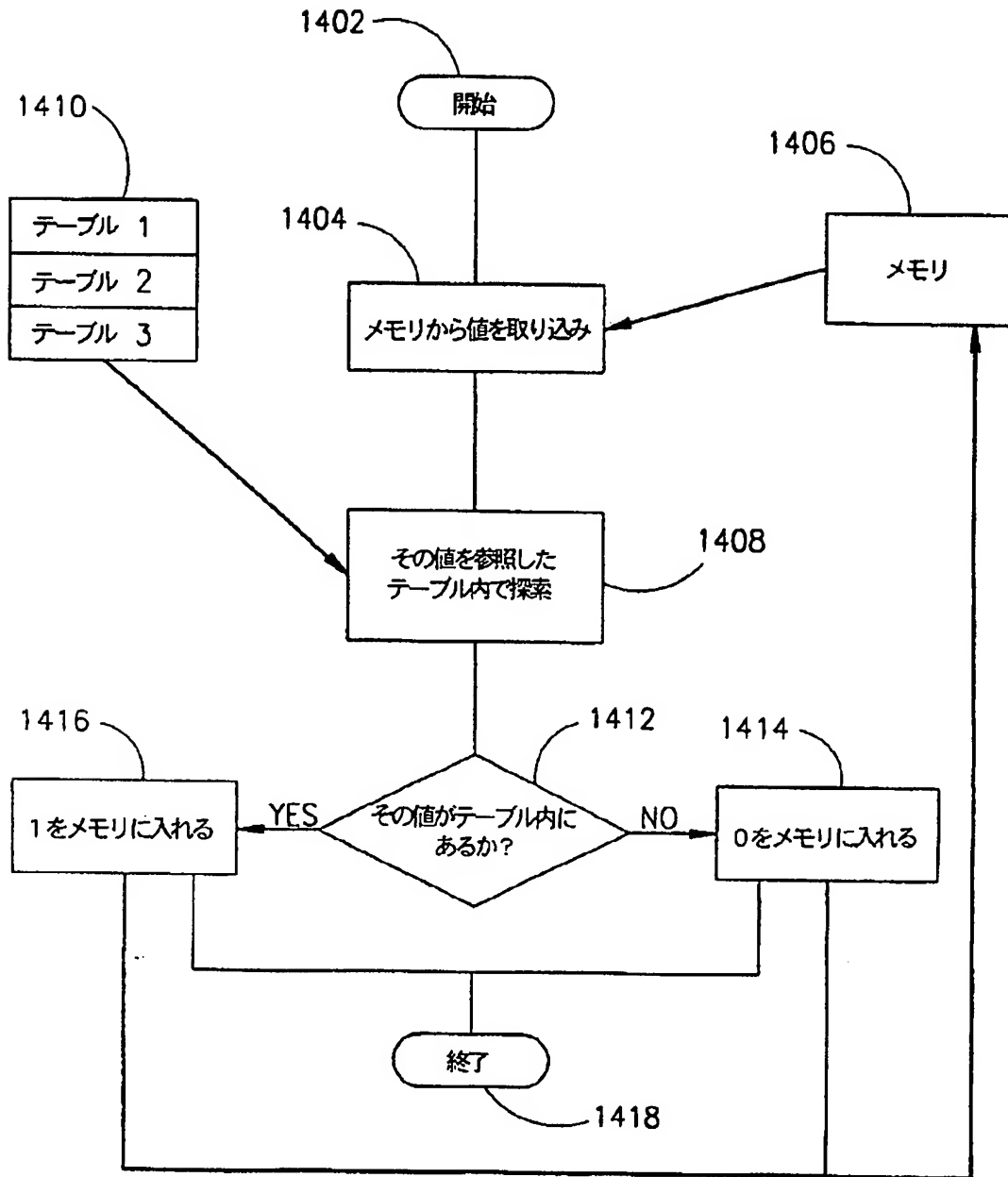


FIG.14

【図15】

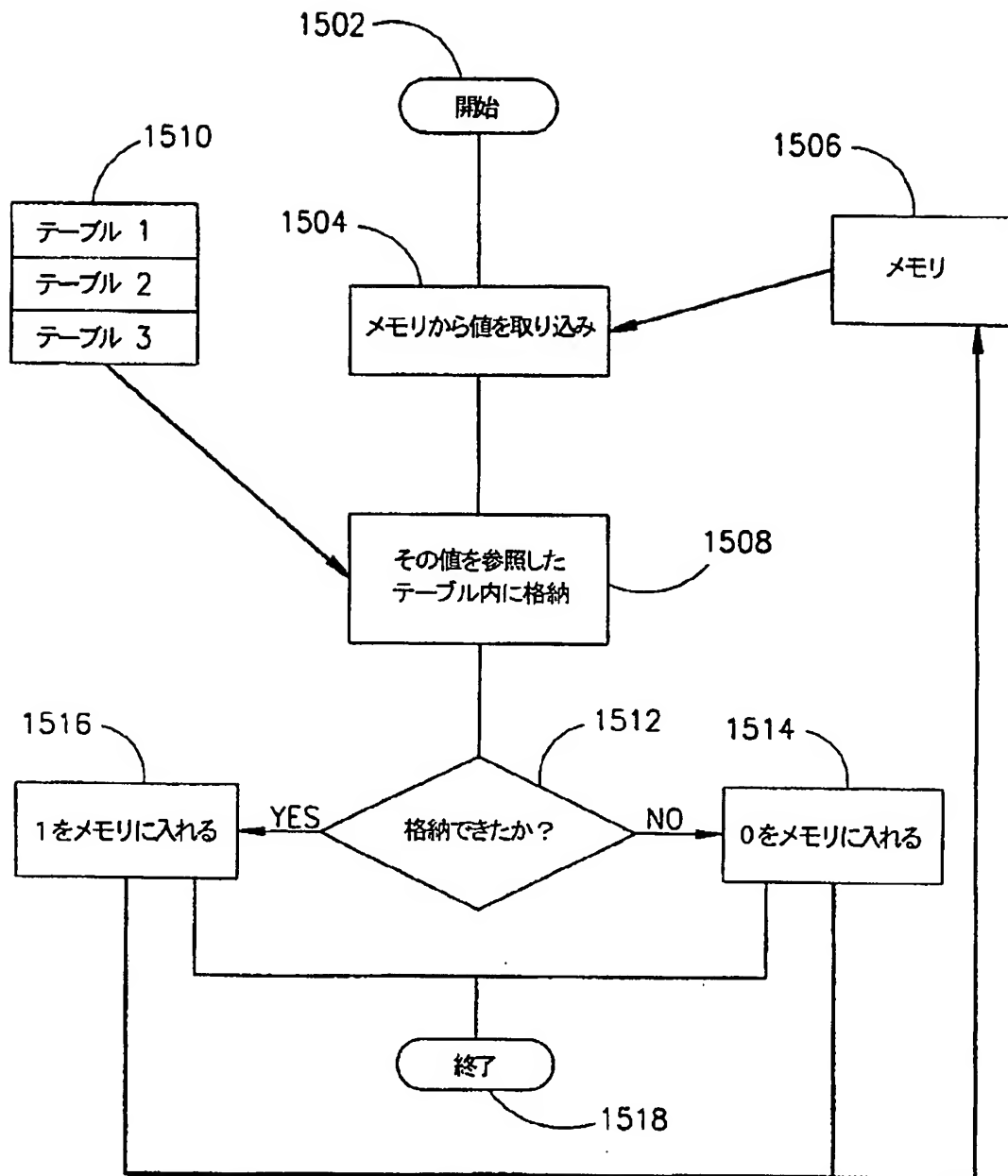


FIG.15

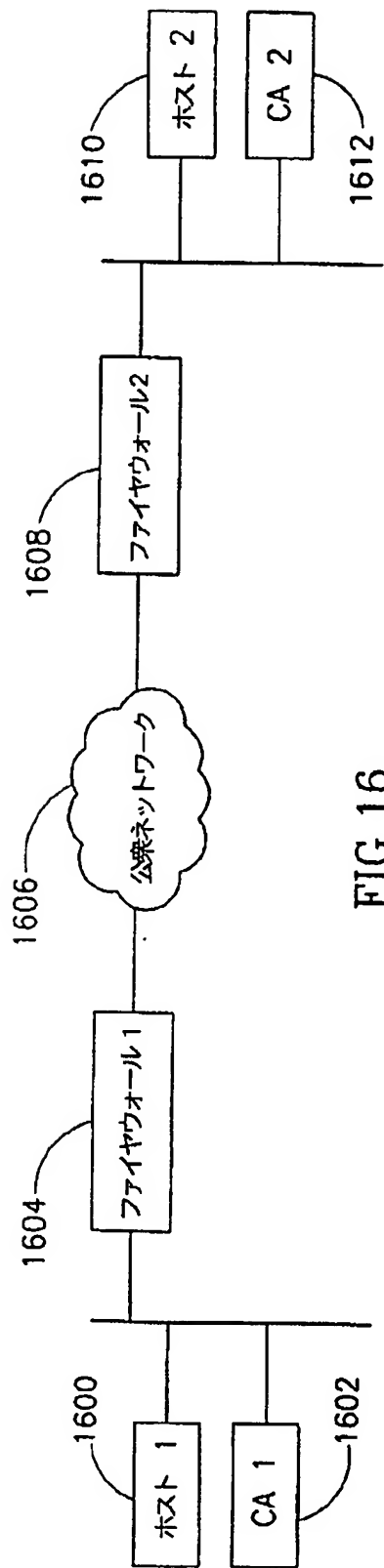


FIG.16

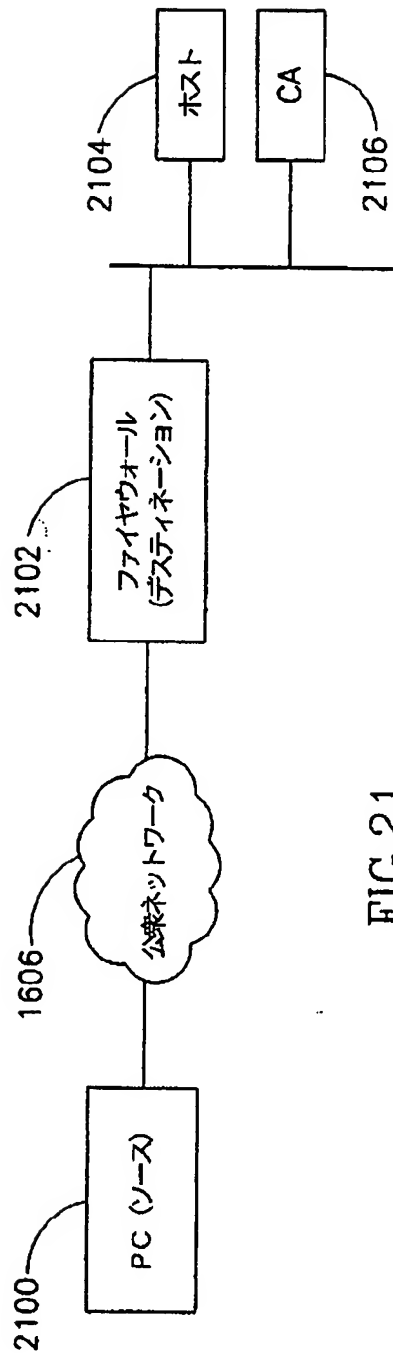


FIG.21

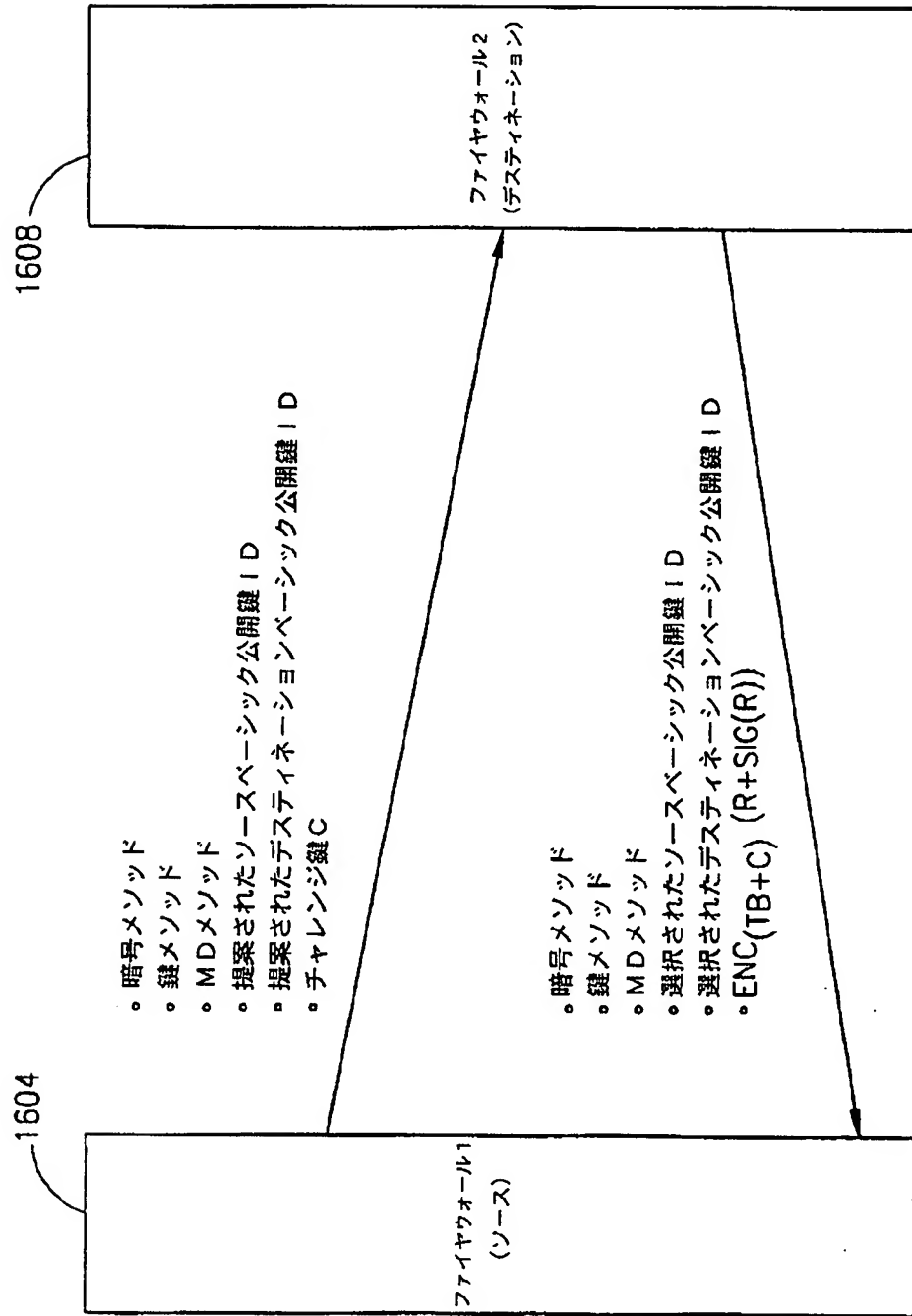


FIG.17

【図18】

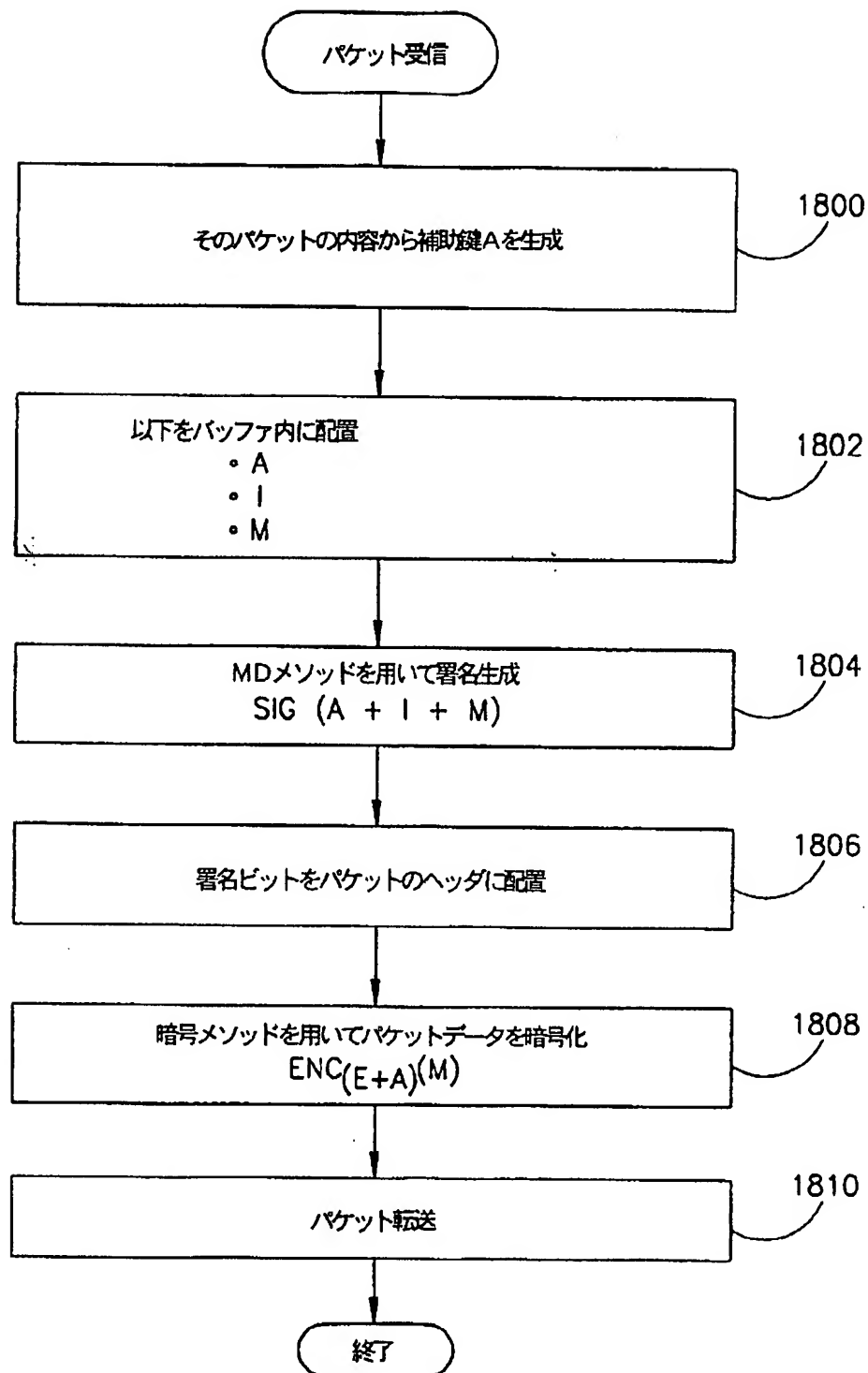


FIG.18

【図19】

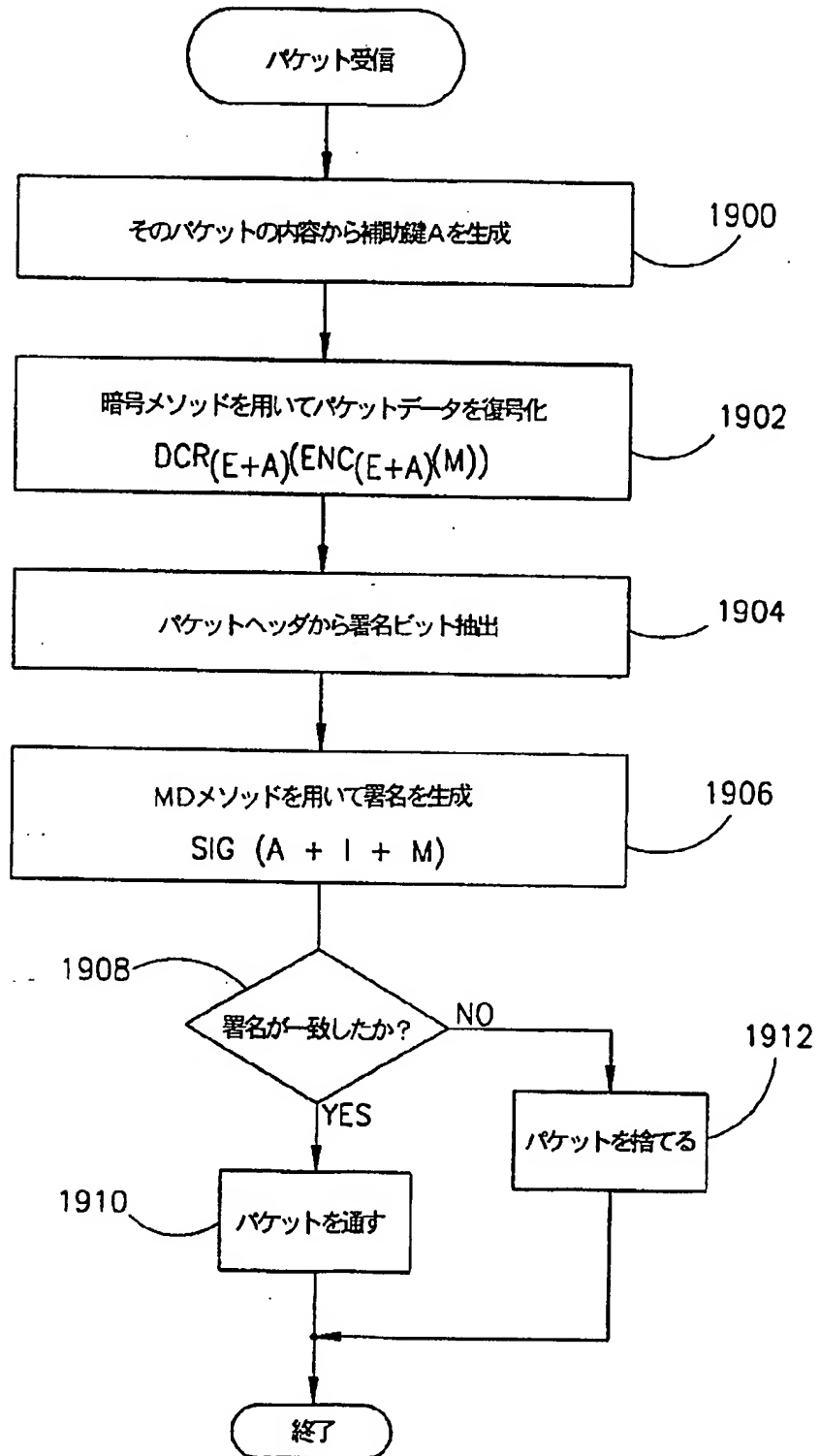


FIG.19

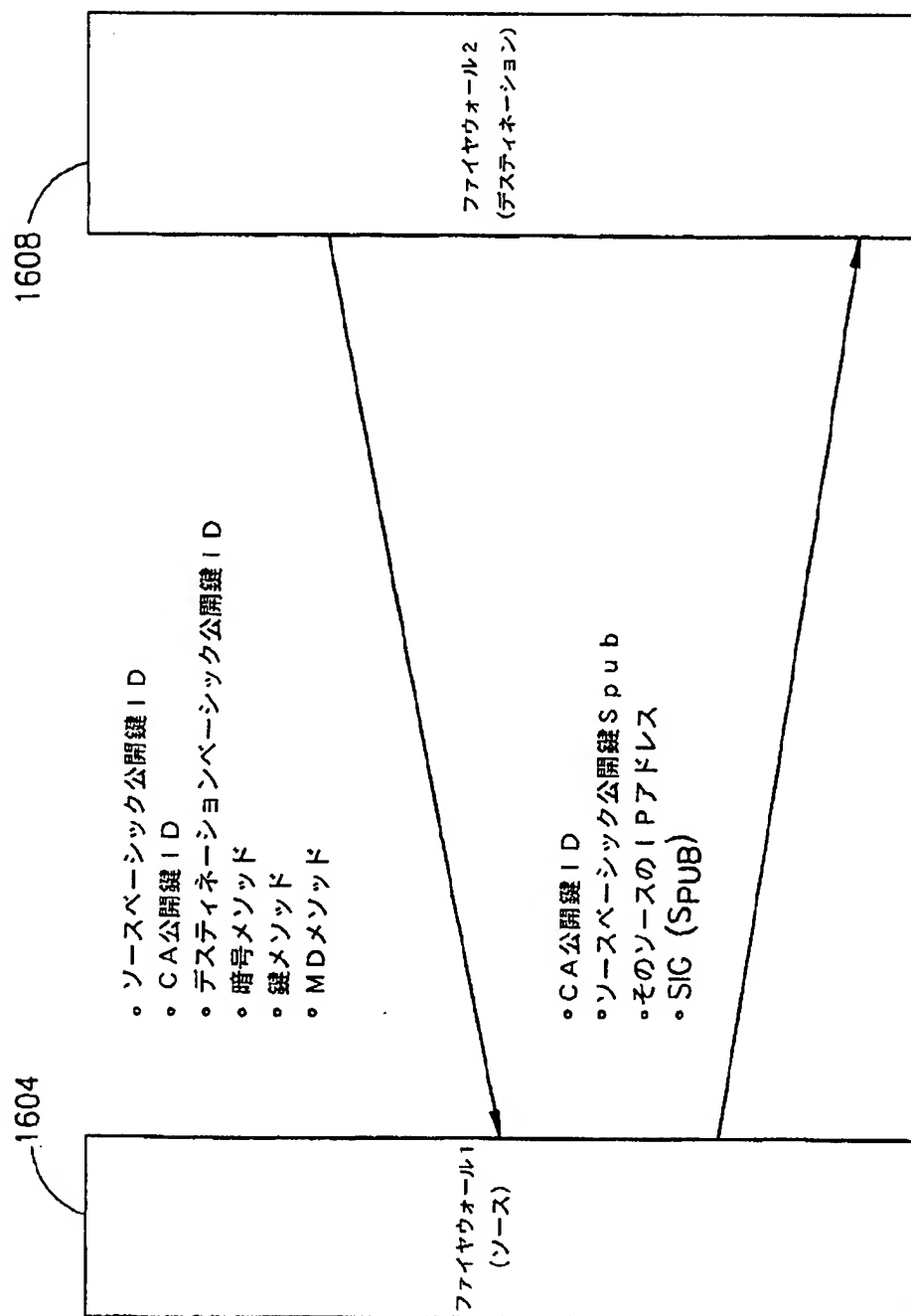


FIG.20

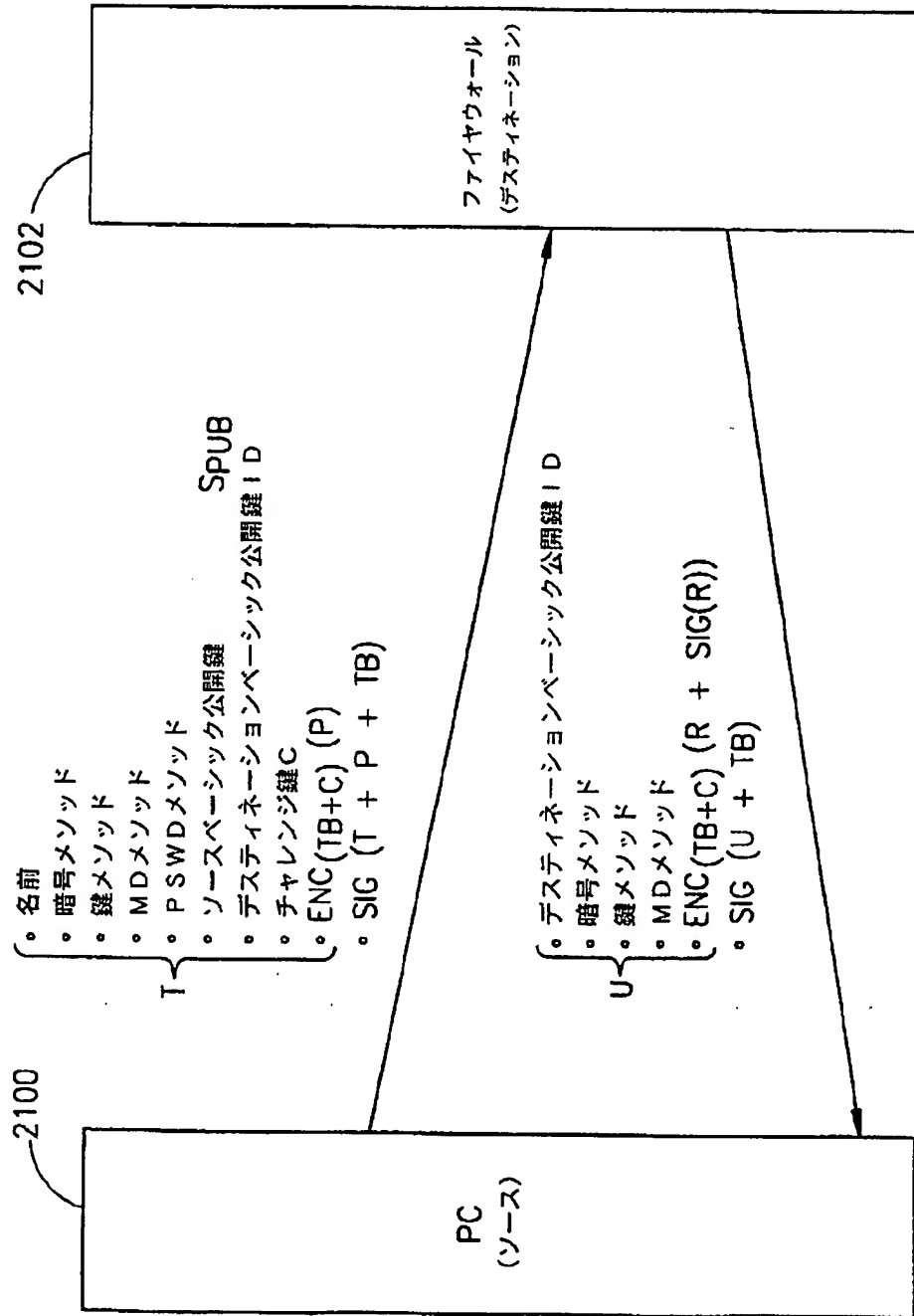


FIG.22

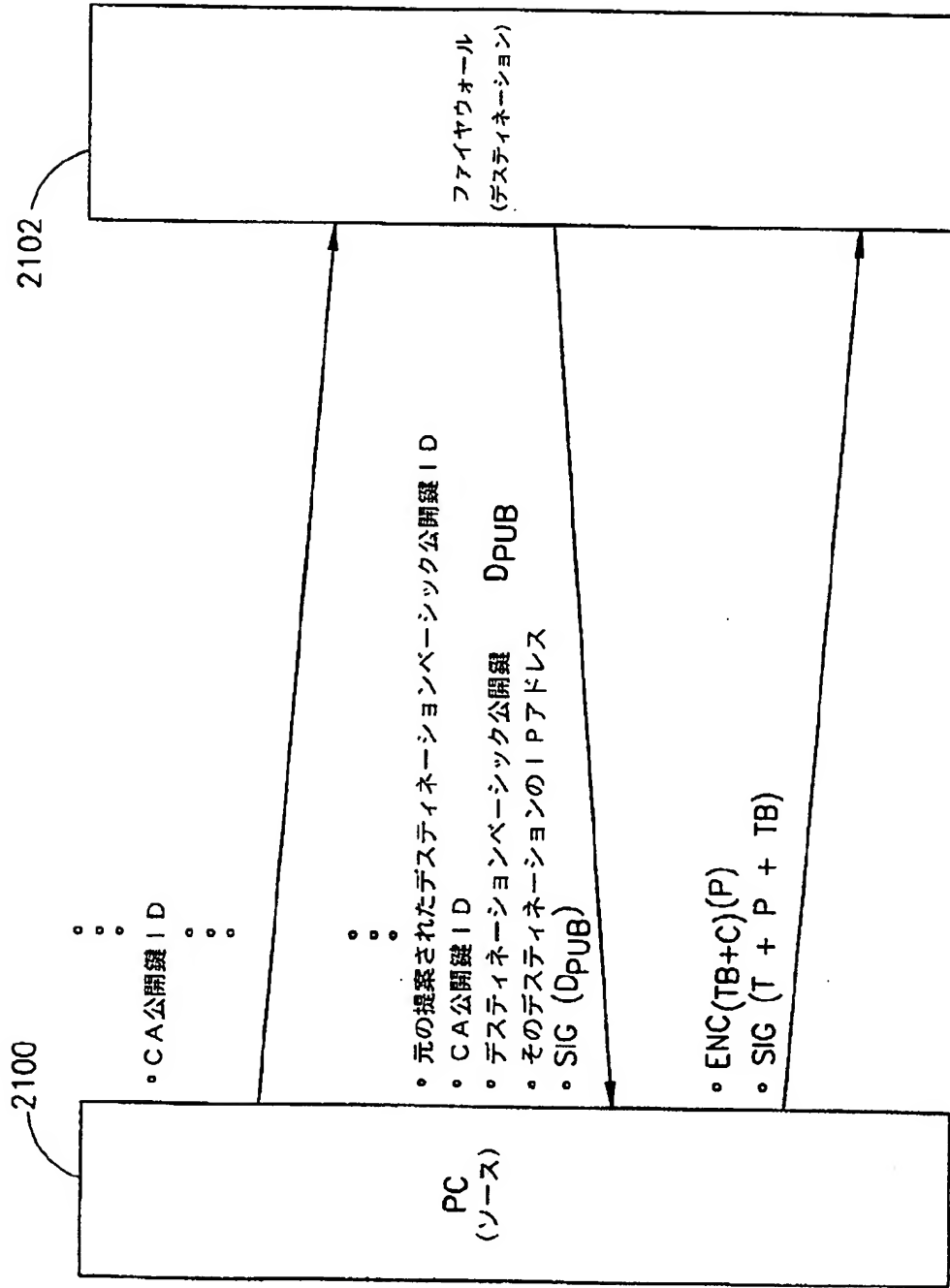


FIG.23

INTERNATIONAL SEARCH REPORT

 International application No.
 PCT/IL96/00017

A. CLASSIFICATION OF SUBJECT MATTER IPC(6) : H04L 9/00, 12/56 US CL : 395/187.01 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) U.S. : 395/187.01, 200.01, 200.06, 200.09, 200.11, 200.17, 200.18; 370/60, 94.1 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) APS		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,247,693 (BRISTOL) 21 September 1993, col. 4, line 43-col. 5, line 33.	1-25
Y, E	US 5,555,346 (GROSS et al.) 10 September 1996, col. 2, line 37-col.3, line 21.	1-25
Y, P	US 5,515,376 (MURTHY et al.) 07 May 1996, col. 2, line 31-col. 3, line 23.	2-5, 10-13, 19-22
Y, P	US 5,473,607 (HAUSMAN et al.) 05 December 1995, col. 3, line 36-col. 4, line 20.	14-16
Y	US 5,329,623 (SMITH et al.) 12 July 1994, col. 2, line 51-col. 3, line 25.	8, 17, 23, 25
A, P	US 5,485,455 (DOBBINS et al.) 16 January 1996, col. 2, line 66-col. 6, line 25.	1, 9, 18, 24
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: *A* document defining the general state of the art which is not considered to be part of particular relevance *E* earlier document published on or after the international filing date *L* documents which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reasons (as specified) *O* document referring to an oral disclosure, use, exhibition or other means *P* document published prior to the international filing date but later than the priority date claimed *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* documents of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* documents of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art *Z* document member of the same patent family		
Date of the actual completion of the international search 10 DECEMBER 1996		Date of mailing of the international search report 31 JAN 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230		Authorized officer STEPHEN C. ELMORE Telephone No. (703) 305-9713

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL96/00017**Box I Observations where certain claims were found unsearchable (Continuation of Item 1 of first sheet)**

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.: 26 (2nd Clm numbered 12)
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

The claim is indefinite in that it fails to point out what is included or excluded by the claim language. This claim is an omnibus type claim.
3. ☒ Claims Nos.: 26 (2nd Clm numbered 12)
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of Item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet(1))(July 1992)★

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(KE, LS, MW, SD, SZ, UG), UA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN

(72)発明者 ズク、ニール

イスラエル国ラマツガン52504・ツビス
トリート 2

(72)発明者 ドゴン、ギル

イスラエル国ヘルツェリア46743・ハキド
マストリート 78

(72)発明者 ベンルーベン、エフド

イスラエル国テルアビブ62486・アルバア
ラトゾットストリート 11

【要約の続き】

ルベースのルールに従ってフィルタリング処理されることになる。前述の検査エンジンは、パケットを受け取るか拒絶するかを各パケット毎に決定する仮想パケットフィルタリングマシンとして機能する。パケットが拒絶される場合、そのパケットは破棄される。パケットが受容される場合、そのパケットは次いで変更処理を施され得る。変更処理には、暗号化、復号化、署名生成、署名確認、またはアドレス変換が含まれ得る。全てのパケット変更処理はルベースの内容に従って実行される。本発明においては、2つのファイヤウォール間、またはクライアントとファイヤウォール間の通信を暗号化することにより、コンピュータネットワークのセキュリティを更に高めている。これにより、私設ネットワーク及び公衆ネットワークを共にその一部として含むWANにおいて、機密保護されていない公衆ネットワークの使用が可能となり、従って、仮想私設ネットワーク(VPN)を形成できることになる。